BİLGİ SİSTEMLERİNİN GÜVENLİĞİNE İLİŞKİN OECD REHBER İLKELERİ- GÜVENLİK KÜLTÜRÜNE DOĞRU

14 Aralık 1960 tarihli İktisadi İşbirliği ve Gelişme Teşkilat Anlaşmasının, özellikle 1b), 1 c), 3 a) ve 5 b) maddeleri uyarınca;

23 Eylül 1980 tarihli Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkelerine yönelik Konsey Önerisi uyarınca;

11 Nisan 1985 tarihinde OECD Üye ülke hükümetlerince kabul edilen Sınır Ötesi Veri Akışı Bildirisi uyarınca [Ek C(85)139];

27 Mart 1997 tarihli Kriptografi Politikası Rehber İlkelerine İlişkin Konsey Önerisi uyarınca [C(97)62/FINAL];

7-9 Aralık 1998 tarihli Küresel Ağlarda Mahremiyetin Korunmasına İlişkin Bakanlar Konseyi Bildirisi uyarınca [Ek C(98)177/FINAL];

7-9 Aralık 1998 tarihli Elektronik Ticaretin Doğrulanmasına İlişkin Bakanlar Konseyi Bildirisi uyarınca[Ek C(98)177/FINAL];

Bilgi sistem ve ağlarının, hükümetler, iş çevreleri, kuruluşlar ve bireysel kullanıcılar tarafından kullanımının ve değerinin giderek arttığını;

Bilgi sistem ve ağlarının ve ulusal ekonomilerin, uluslar arası ticaretin ve sosyal, kültürel ve siyasi yaşamın dengeli ve verimli işleyişi açısından giderek daha fazla önem kazanması nedeniyle söz konusu bilgi sistem ve ağların güvenilirliğinin korunması ve kuvvetlendirilmesi ihtiyacını;

Bilgi sistem ve ağlarının dünya çapında kullanımının beraberinde yeni ve artan oranda riskler getirdiğini;

Yetkisiz erişim ve kullanım, kötü kullanım, değiştirilme, kötü amaçlı kod iletimleri, hizmetteki aksaklık ya da tahribatlar karşısında bilgi sistem ve ağları aracılığıyla iletilen ve kaydedilen veri ve bilgilerin tehdit altında olduğu ve uygun korunma yöntemlerine ihtiyaç duyulduğunu;

Bilgi sistem ve ağlarına yönelik riskler ve bu risklerle ilgili politikalar, uygulamalar, önlemler ve prosedürler hakkında bilincin artması gerektiği ve bir güvenlik kültürünü geliştirmek için uygun tutum ve davranışların teşvik edilmesi gereksinimini;

Bilgi sistem ve ağlarına yönelik tehditlerden doğan zorluklara karşı hazırlıklı olmak için mevcut politika, uygulama, önlem ve prosedürlerin gözden geçirilmeleri gereksinimini;

Güvenlik eksiklikleri sebebiyle ulusal ekonomilerin, uluslar arası ticaretin, sosyal, kültürel ve siyasi yaşamdaki katılımın karşı karşıya olduğu potansiyel hasarların yarattığı zorluklarla mücadele etmek için uluslararası eşgüdüm ve işbirliğini kuvvetlendiren bir güvenlik kültürü aracılığıyla bilgi sistem ve ağlarının güvenliğini teşvik etmenin ortak çıkarların gereği olacağını;

Bu Öneri Ekinde yer alan *Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkelerin* ulusların egemenlik haklarını etkilemediği ve isteğe bağlı olduğunu;

Rehber İlkelerin amacının güvenlik hususunda tek ve kesin bir çözüm ileri sürmek ya da belli bir durumda hangi politika, uygulama, önlem ve prosedürlerin uygun olduğu hususunda net bir açıklama getirmek olmadığı, daha ziyade kullanıcıların bir güvenlik kültürünü nasıl oluşturacağı ve aynı zamanda ondan nasıl yararlanacağı konusunda daha iyi bir anlayış yerleştirmek üzere çerçeve ilkeler sunmak olduğunu

GÖZ ÖNÜNE ALARAK;

KONSEY,

Bilgi sistem ve ağlarını geliştiren, sahip olan, yöneten, hizmete sunan ve kullanan hükümetler, iş çevreleri, diğer örgütler ve bireysel kullanıcılar için *Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeler: Güvenlik Kültürüne Doğru* adlı ilkeleri

ÖNERMEKTEDİR.

Üye ülkelerin;

Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeler: Güvenlik Kültürüne Doğru adlı ilkeler uyarınca bir güvenlik kültürünü benimseyerek ve teşvik ederek mevcut politika, uygulama, önlem ya da prosedürlerini değiştirmelerini ya da yenilerini oluşturmalarını;

Rehber İlkeleri uygulamak için ulusal ve uluslar arası düzeyde işbirliği yapmalarını, koordinasyon sağlamalarını;

Güvenlik kültürünü teşvik etmek ve tüm kullanıcıları sorumluluk alarak Rehber İlkelerini kendilerine düşen rollere uygun bir şekilde uygulamak amacıyla gerekli adımları atmaya teşvik etmek için Rehber İlkelerini hükümetler, iş çevreleri, diğer örgütler ve bireysel kullanıcılar da dahil olmak üzere tüm kamu ve özel sektöre dağıtmalarını;

Üye olmayan ülkelere zamanında ve uygun bir şekilde Rehber İlkeleri tanıtmalarını;

Bilgi sistem ve ağlarının güvenliği ile ilgili konularda uluslar arası işbirliğini kuvvetlendirmek için her beş yılda bir Rehber İlkeleri gözden geçirmelerini

TAVSİYE ETMEKTEDİR

Ve

OECD Bilişim, Bilgisayar ve İletişim Politikası Komitesini Rehber İlkelerin uygulanmasını teşvik etmekle

GÖREVLENDİRMEKTEDİR.

Bu Öneri, Bilgi Sistemlerinin Güvenliği için Rehber İlkeler başlıklı 26 Kasım 1992 tarihli Önerinin [C(92)188/FINAL]yerine geçmektedir.

EK

BİLGİ SİSTEMLERİNİN GÜVENLİĞİNE İLİŞKİN OECD REHBER İLKELERİ- GÜVENLİK KÜLTÜRÜNE DOĞRU

ÖNSÖZ

1. *Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkelerin* ilk kez 1992'de OECD tarafından yayınlanmasından günümüze kadar, bilgi sistemleri ve ağlarının kullanılması ve tüm bilgi teknolojileri büyük ölçüde değişime uğramıştır. Devam edegelen bu değişiklikler önemli avantajlar sunmakla birlikte, aynı zamanda bilgi sistemlerini ve ağlarını kullanan, geliştiren, sahip olan, yöneten, sağlayan, sunan ve kullanan hükümetler, iş çevreleri, diğer örgütler ve bireylerin ("kullanıcılar") güvenlik hususuna daha fazla dikkat etmelerini gerektirmektedir.

2. Daha güçlü kişisel bilgisayarlar, ilerleyen teknolojiler ve internetin geniş kapsamlı kullanımı, kapalı ağlardaki basit ve tek başına işletilen sistemlerin yerini almıştır. Günümüzde, kullanıcılar giderek artan oranda birbirine bağlanmakta ve bu bağlantılar ulusal sınırları aşmaktadır. Ayrıca internet enerji, ulaştırma ve finans gibi önemli altyapıları da desteklemekte olup, şirketlerin işleyişinde, hükümetlerin vatandaşlara ve teşebbüslere sundukları hizmetlerde ve bireylerin iletişim ve bilgi alışverişinde önemli bir rol oynamaktadır. İletişim ve bilgi altyapısını oluşturan teknolojilerin yapısı ve çeşidi de oldukça değişmiştir. Altyapı erişim araçlarının sayısı ve yapısı sabit, kablosuz ve mobil araçları kapsayacak şekilde çoğalmıştır. Erişim, artık artan bir oranda sürekli çevrimiçi olan bağlantılar aracılığıyla yapılmaktadır. Sonuç olarak bilgi alışverişinin doğası, hacmi ve hassasiyeti büyük ölçüde artmıştır.

3. Bilgi sistemleri ve ağlarının birbirleri ile bağlantısındaki artışın sonucu olarak, bilgi sistemleri ve ağlarının güvenliği artık artan sayıda ve çeşitlilikte tehditlere maruzdur. Bu durum güvenlik açısından yeni konuları gündeme getirmektedir. Bu nedenlerle, bu Rehber İlkeler, yeni bilgi toplumunda yer alan tüm kullanıcılara yöneliktir ve güvenlik konularının

daha bilinçli olarak ele alınmasının ve bir "güvenlik kültürü"nü geliştirmenin gereğini vurgulamaktadır.

I. GÜVENLİK KÜLTÜRÜNE DOĞRU

4. Bu Rehber İlkeler, sürekli değişen güvenlik ortamına güvenlik kültürünün geliştirilmesini teşvik etmek suretiyle cevap vermektedir-yani, bilgi sistem ve ağlarının geliştirilmesinde güvenlik hususuna dikkat edilmesini ve bilgi sistem ve ağlarını kullanırken yeni düşünme ve davranış yöntemlerinin benimsenmesini önermektedir. Rehber İlkeler, sistem ve ağların güvenliğinin tasarımını ve kullanımını genelde daha sonra ele alan eski yöntemi geride bırakmaktadır. Kullanıcının, bilgi sistemleri, ağlar ve ilgili hizmetlere daha bağımlı hale gelmesinden dolayı bu sistemlerin güvenli olması gerekmektedir. Sadece tüm kullanıcıların çıkarları ile sistem, ağ ve ilgili hizmetlerin doğasını göz önünde bulunduran bir yaklaşım etkili bir güvenlik sağlayabilir.

5. Güvenliği sağlamak açısından her kullanıcı önemli bir unsurdur. Kullanıcılar, rolleri gereği karşı karşıya oldukları güvenlik riskleri ve önleyici tedbirlerden haberdar olmalı, sorumluluk almalı ve bilgi sistem ve ağlarının güvenliğini artırmak için gerekli adımları atmalıdır.

6. Güvenlik kültürünün geliştirilmesi hem liderlik hem de geniş kapsamlı bir katılım gerektirmekte, bu da, tüm kullanıcılar arasında güvenliğin sağlanması konusundaki anlayış kadar, güvenlik planlaması ve yönetimine de öncelik tanınması sonucunu doğurmaktadır. İdarenin tüm seviyeleri, iş çevreleri ve tüm kullanıcılar, güvenlik konularında sorumluluk almalıdır. Bu Rehber İlkeler, toplum aracılığıyla bir güvenlik kültürü oluşturmak için gerekli temeli sağlamaktadır. Böylelikle kullanıcılar, güvenlik unsurunu bilgi sistemleri ve ağlarının kullanımı ve tasarımına dahil edebilirler. Rehber İlkeler, tüm kullanıcıların, bilgi sistem ve ağlarıyla ilgili işlemlerde güvenlik kültürünü bir düşünce, değerlendirme ve faaliyet yöntemi olarak benimsemesini ve teşvik etmesini önermektedir.

II. AMAÇLAR

7. Bu Rehber İlkeler;

- Bilgi sistem ve ağlarının koruma aracı olarak tüm kullanıcılar arasında güvenlik kültürünü teşvik etmeyi,

- Bilgi sistemleri ve ağlarının karşı karşıya olduğu riskler ve bu risklere karşı mevcut politikalar, uygulamalar, önlemler ve prosedürlerle ilgili bilinci arttırmak ve bu yöntemlerin uygulanmasının gerekliliğini vurgulamayı,

- Bilgi sistemleri ve ağları ile bunların sunum ve kullanım yöntemleri konusunda tüm kullanıcıların güvenini artırmayı,

- Bilgi sistemlerinin ve ağlarının güvenliğine yönelik uyumlu politika, uygulama, önlem ve prosedürlerin geliştirilmesi ve uygulanması ile ilgili etik değerlere kullanıcılar tarafından saygı gösterilmesi ve güvenlik konularının iyi anlaşılmasına yardımcı olacak genel bir referans çerçevesi oluşturulmasını,

- Güvenlik politikalarının, uygulamalarının, tedbir ve prosedürlerinin geliştirilmesi ve uygulanması açısından tüm kullanıcılar arasında işbirliği ve bilgi paylaşımını teşvik etmeyi,

- Standartların geliştirilmesi ve uygulanmasında rol alan tüm kullanıcıların güvenlik konusunu önemli bir hedef olarak belirlemelerini teşvik etmeyi

amaçlamaktadır.

III.İLKELER

8. Aşağıda sayılan dokuz ilke birbirini tamamlayıcı nitelikte olup, bir bütün olarak okunmalıdır. İlkeler, politika ve uygulama seviyeleri de dahil olmak üzere tüm kullanıcıları ilgilendirmektedir. Bu Rehber İlkeler çerçevesinde kullanıcıların sorumlulukları rollerine göre değişiklik göstermektedir. Daha sağlam bir güvenlik anlayışının yerleşmesi ve uygulamaların benimsenmesi için eğitim, bilgi paylaşımı ve öğretim sayesinde tüm kullanıcılara yardımcı olunacaktır. Bilgi sistemleri ve ağlarının güvenliğini artırma çabaları, demokratik toplum

değerleri ile, özellikle de kişisel mahremiyet ile ilgili temel konular ve bilginin açık ve serbest akışı gereksinimi ile uyumlu olmalıdır. [1]

1) Bilinç

Kullanıcılar, bilgi sistemleri ve ağlarının güvenliğinin gerekliliği ve güvenliği artırmak için neler yapabilecekleri konularında bilinçli olmalıdır.

Bilgi sistemleri ve ağlarının güvenliği açısından, riskler ve mevcut korunma yöntemleri konularındaki bilinç ilk savunma adımını oluşturmaktadır. Bilgi sistem ve ağları hem iç hem de dış risklerden etkilenebilir. Kullanıcılar güvenlik konusundaki eksikliklerin kontrolleri altındaki sistem ve ağlara büyük ölçüde zarar verebileceğini bilmeli, birbirine bağlı ve bağımlı olan sistemler nedeniyle diğer kullanıcılara da zarar verebileceklerini unutmamalıdırlar. Kullanıcılar, sistemlerinin konfigürasyonu, güncelleştirilmesi ve ağ içindeki yeri ile güvenliği artırmak için uygulayabilecekleri iyi örnekler ve diğer kullanıcıların gereksinimleri konularında bilgi sahibi olmalıdır.

2) Sorumluluk

Tüm kullanıcılar bilgi sistem ve ağlarının güvenliğinden sorumludur.

Yerel ve küresel bilgi sistemlerine ve ağlarına bağlı olan kullanıcılar, sistem ve ağların güvenliği hususunda kendilerine düşen sorumlulukların farkında olmalıdır. Kendilerine düşen rollere uygun bir şekilde davranmalıdırlar. Kullanıcılar kendi politika, uygulama, önlem ve prosedürlerini düzenli olarak incelemeli ve uygun olup olmadıklarını değerlendirmelidir. Ürün ve hizmet sağlayan, geliştiren ve tasarlayan kullanıcılar, kullanıcıların ürün ve hizmetlerin güvenlik fonksiyonlarını daha iyi anlayabilmeleri ve bu konuda kendi sorumluluklarının bilincine varabilmeleri için sistem ve ağ güvenliği konusunu dikkate almalı ve güncelleme dahil gerekli bilgileri sunmalıdır.

3) Tepki

[1] Bu Güvenlik Rehber İlkelerine ek olarak OECD dünya bilgi toplumu açısından önemli olan diğer konularda da tamamlayıcı nitelikte tavsiyelerde bulunmuştur. Bu tavsiyeler, mahremiyet (1980 tarihli OECD Mahremiyetin Korunması ve Kişisel Bilgilerin Sınırlararası Akışına Yönelik Rehber İlkeler) ve kriptografi (1997 tarihli OECD

Kullanıcılar, güvenlik tehditlerini önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmelidir.

Kullanıcılar, bilgi sistem ve ağlarının birbirlerine bağlı olan yapısı ve potansiyel hasarların hızla ve geniş kapsamda yayılabileceğini göz önüne alarak, güvenlikle ilgili tehditler karşısında işbirliği içinde olmalı ve zamanında müdahale etmeli; tehdit ve zayıf noktalar konusundaki bilgileri mümkün olduğunca paylaşmalı, güvenlik tehditlerini önlemek, saptamak ve müdahale etmek amacıyla hızlı ve etkili bir işbirliği sağlamak için gerekli prosedürleri uygulamalıdırlar. İzin verildiği durumlarda sınır aşan bilgi paylaşımı ve işbirliği de buna dahil edilebilir.

4) Etik

Kullanıcılar birbirlerinin yasal çıkarlarına saygı göstermelidir.

Bilgi sistem ve ağlarının toplumumuzda ne kadar hızlı yaygınlaştığı düşünülürse, kullanıcıların eylemlerinin veya tepkisizliklerinin diğerlerine zarar verebileceğini bilmeleri gerekmektedir. Bu sebeple ahlaki davranışlar çok önemli olup; kullanıcılar en iyi uygulamaları geliştirmeye ve benimsemeye özen göstermeli, güvenlik ihtiyaçlarını göz önünde bulunduran davranışları teşvik ederek, diğer tarafların çıkarlarına saygı göstermelidir.

5) Demokrasi

Bilgi sistem ve ağlarının güvenliği, demokratik toplumun temel değerleri ile uyumlu olmalıdır.

Güvenlik uygulamaları, düşünce ve ifade özgürlüğü, bilginin serbest akışı, bilgi ve iletişimin güvenilirliği, kişisel bilginin korunması, açıklık ve şeffaflık gibi demokratik toplumlardaki değerler ile uyumlu bir şekilde yürütülmelidir.

6) Risk değerlendirmesi

Kriptografi Politikasına Yönelik Rehber İlkeler) ile ilgilidir. Güvenlik Rehber İlkeleri bu tavsiyeler ile birlikte okunmalıdır.

Kullanıcılar risk değerlendirmeleri yapmalıdır.

Tehdit ve hassasiyetleri tanımlayan risk değerlendirmeleri, teknoloji, fiziksel ve insani etkenler, politikalar ve üçüncü taraf hizmetleri gibi önemli iç ve dış faktörleri kapsayacak şekilde geniş bir tabana teşmil edilmelidir. Risk değerlendirmeleri kabul edilebilir risk seviyesinin belirlenmesini sağlar ve korunması gereken bilginin yapısı ve önemi doğrultusunda, bilgi sistem ve ağlarının karşı karşıya olduğu potansiyel zarar risklerini yönetmek için gerekli kontrollerin seçilmesine yardımcı olur. Bilgi sistemlerinin giderek daha bağlı bir hale gelmeleri nedeniyle risk değerlendirmeleri, diğer kullanıcılardan kaynaklanan ya da onları etkileyebilecek potansiyel hasarları da göz önüne almalıdır.

7) Güvenlik tasarımı ve uygulama

Kullanıcılar, güvenliği, bilgi sistem ve ağlarının önemli bir unsuru olarak ele almalıdır.

Güvenliği optimum kılmak için sistemler, ağlar ve politikalar uygun şekilde tasarlanmalı, uygulanmalı ve koordine edilmelidir. Bu çabaların önemli bir parçası da, tanımlanmış tehdit ve hassasiyetlerden kaynaklanabilecek potansiyel hasarları engellemek ya da en aza indirmek için uygun korunma yöntemleri ve çözümlerinin tasarlanması ve benimsenmesidir. Hem teknik hem de teknik olmayan korunma yöntemleri ve çözümleri gerekmekte olup, bunlar, organizasyonun sistem ve ağlarında bulunan bilginin değeri ile orantılı olmalıdır. Güvenlik, ürün, hizmet, sistem ve ağların temel bir unsuru olmalı ve sistem tasarımı ve mimarisinin bölünmez bir parçası haline gelmelidir. Uç kullanıcılar için güvenlik tasarımı ve uygulanışı genelde kendi sistemleri için ürün ve hizmetleri seçmek ve yapılandırmak anlamına gelmektedir.

8) Güvenlik Yönetimi

Kullanıcılar güvenlik yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.

Güvenlik yönetimi, risk değerlendirmesine dayalı ve kullanıcıların tüm faaliyet düzeylerini ve işlemlerinin her safhasını kapsayacak şekilde dinamik olmalıdır. Yeni tehditlere karşı ileri görüşlü çözümler içermeli, sistem onarımı, bakım, inceleme ve arızalara karşı önlem, saptama ve müdahale gibi konulara dikkat etmelidir. Bilgi sistem ve ağ güvenlik politikaları, uygulamaları, önlemleri ve prosedürleri tutarlı bir güvenlik sistemi oluşturmak için koordine edilmeli ve bütünleştirilmelidir. Güvenlik yönetimi gereksinimleri, katılım seviyesine, kullanıcının rolüne, riske ve sistem gereksinimlerine bağlıdır.

9) Yeniden değerlendirme

Kullanıcılar bilgi sistem ve ağlarının güvenliklerini incelemeli ve yeniden değerlendirmeli; güvenlik ile ilgili politika, uygulama, önlem ve prosedürlerde gerekli değişiklikleri yapmalıdır.

Sürekli olarak yeni ve değişen tehdit ve hassasiyetler ortaya çıkmaktadır. Kullanıcılar, değişen bu riskler ile mücadele etmek için güvenliğin tüm unsurlarını devamlı olarak incelemeli, yeniden değerlendirmeli ve değiştirmelidir.