OECD Dijital Ekonomi Politikası Belgesi

Ekonomik ve Sosyal Refah için Dijital Güvenlik Risk Yönetimi

OECD Tavsiye Metni ve Yardımcı El Kitabı

2016

Ekonomik ve Sosyal Refah için Dijital Güvenlik Risk Yönetimi

OECD Tavsiye Metni ve Yardımcı El Kitabı

T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

TELİF HAKKI

AÇIKLAMA

Bu belge ve belgede kullanılan her türlü harita herhangi bir bölgenin statüsü ya da hükmü üzerine, uluslararası sınırların oluşturulmasına ve herhangi bir ülkenin, şehrin ya da bölgenin ismine karşı önyargısı bulunmamaktadır.

OECD yayınlarındaki düzeltmeler İnternet üzerinden aşağıdaki adreste bulunmaktadır:

www.oecd.org/publishing/corrigenda.

ÖNSÖZ

OECD *Ekonomik ve Sosyal Refah için Dijital Güvenlik Risk Yönetimi Tavsiye Metni* ve buna ek Yardımcı El Kitabı, dijital açıklıktan beklenen ekonomik ve sosyal faydaların optimize edilmesini hedeflemek adına, yeni nesil ulusal dijital güvenlik risk yönetimi stratejilerinin oluşturulmasında rehberlik sağlamaktadır.

Son yıllarda dijital güvenlik tehditleri ve vakaların sayısı artmış, bu da kamu ve özel sektör kurumları ile bireyler için önemli ekonomik ve sosyal sonuçlara neden olmuştur. Bunlara örnek olarak işlerin aksatılması (hizmet engelleme ya da sabotaj gibi yollarla), doğrudan maddi zarar, davalar, itibar kaybı, rekabetçiliğin zarar görmesi (ticari sır hırsızlığı gibi vakalarla) ve müşteri güveni kaybı gibi durumlar gösterilebilir. Giderek daha fazla sayıda paydaş, dijital ekonominin getirilerinden faydalanmak için daha iyi bir dijital güvenlik risk yönetiminin gerekliliğinin farkına varmaktadır.

Son otuz yıldır OECD, dijital ekonomide yenilikçilik ve güven için politikaların ve araçların öne çıkarılmasında önemli rol oynamıştır. Bu Tavsiye Metninin OECD Konseyi tarafından 17 Eylül 2015'te benimsenmesi, 2012'de OECD Dijital Ekonomide Güvenlik ve Gizlilik Çalışma Gurubu (SPDE) tarafından *2002 Bilişim Sistemleri ve Ağlarının Güvenliğine dair Ana Esaslar için Konsey Tavsiyeleri: Güvenlik Kültürüne Doğru* ("Güvenlik Ana Esasları") metninin gözden geçirilmesi ile başlatılan ve birçok paydaşın birlikte hareket etmesi ile ortaya çıkan başarılı bir neticedir.

Devlet güvenlik politikalarını yapanları, iş ve sanayi dünyasını ve İnternet teknolojisiyle ilgilenen toplulukları barındıran bu girişim, SPDE başkanı Jane Hamilton (Kanada) liderliğinde ve Büro'nun aktif desteği ile bir araya getirilmiştir. OECD ve diğer ortak ekonomilerden temsilciler, OECD İş ve Sanayi Danışma Komitesi (BIAC), Sivil Toplum Bilişim Toplumu Danışma Kurulu (CSISAC), İnternet Teknik Danışma Kurulu (ITAC) bu girişimde aktif olarak yer almışlardır. Revize edilmiş Tavsiye Metni son olarak OECD Konseyinde kabul edilmeden önce, 25 Haziran 2015'te Dijital Ekonomi Politikaları Konseyi tarafından tartışılmış ve onaylanmıştır.

Tavsiye Metni devlet yönetimindeki ve kamu ve özel sektör kurumlarındaki en üst düzey liderlere dijital güvenlik risk yönetimine, ekonomik ve sosyal refah adına güven inşa eden ve açık elektronik ortamdan faydalanmayı hedefleyen bir yaklaşımı benimsemeleri üzerine çağrıda bulunmaktadır. Bu yaklaşım, birbiriyle ilişkili, birbirine bağlı ve tamamlayıcı sekiz üst düzey İlkenin oluşturduğu uyumlu bir çerçevede yansıtılmaktadır.

Tavsiye Metni boyunca iki ana mesaj sürekli öne çıkmaktadır.

İlk olarak, kamu ve özel sektör kurumlarının ekonomik ve sosyal hedeflerine ve risk yönetimine dayanan bir yaklaşımın ihtiyacına odaklanılmıştır. Dijital risk, teknik çözümler gerektiren teknik bir sorundan ziyade ekonomik risk olarak ele alınmalıdır; buna bağlı olarak da kurumların genel risk yönetimi ve karar alma mekanizmalarının bir parçası olarak yer almalıdır. Dijital güvenlik riskinin diğer risk kategorilerinden temel olarak farklı türde müdahale gerektirdiği fikrine karşı çıkılması gerekmektedir. Bununla ilintili olarak "siber-güvenlik" terimi ve daha genel olarak bu özel durum havasını veren ve yanlış yönlendirici bir terim olan "siber" ön eki 2015 Tavsiye Metninde kullanılmamıştır.

İkinci olarak, dinamik yönetim ile güvenlik riskinin ilgili faaliyetlerden beklenen ekonomik faydalarına ilişkili olarak kabul edilebilir düzeylere indirilebileceği konusu üzerinde bir uzlaşı vardır. Bu bağlamda dijital güvenlik önlemleri, başkalarının çıkarlarını dikkate alacak, karşı karşıya olunan riske uygun ve orantılı olarak ve korunması hedeflenen ekonomik ve sosyal faaliyetleri engellemeyecek şekilde oluşturulmalıdır.

Bu kitapçık, Tavsiye Metninin yanında, metin ile ilintili olarak hazırlanmış ama onun parçası olmayan, açıklayıcı ve aydınlatıcı nitelikteki Yardımcı El Kitabını da içermektedir. Yardımcı El Kitabı, Tavsiye Metninde önemi vurgulanan ana kavramları ele almakta, ileri sürülen İlkelerin farklı paydaşlar üzerinde uygulanabilirliği hakkında yorumlar bulundurmakta ve netice itibariyle Tavsiye Metninde belirtilen her İlke için açıklama sunmaktadır.

Tavsiye Metninin uygulamaya konması ile dijital risk yönetimine daha bütünsel bir kamu politikası yaklaşımının teşvik edilmesi ve yerel, bölgesel ve uluslararası düzeyde hem devlet yönetimi içinde hem de sivil toplum paydaşları ile beraber yeni koordinasyon mekanizmalarının kurulmasının yanında, kamu ile özel sektör kurumlarının işbirliğinin güçlenmesi de beklenmektedir.

Ekonomik ve Sosyal Refah için Dijital Güvenlik Risk Yönetimi Konsey Tavsiye Metni

17 Eylül 2015 – C(2015)115

14 Aralık 1960 tarihli Ekonomik Kalkınma ve İşbirliği Örgütü Anlaşmasının özellikle 1 b), 1 c), 3 a), 3 b) ve 5 b) maddeleri **UYARINCA;**

Gizliliğin Korunması ve Kişisel Verilerin Sınırlar arası Akışına İlişkin Yönerge ile ilgili Konsey Tavsiyesi ("OECD Gizlilik Yönergesi")[düzenlenmiş haliyle C(80)58/FİNAL]; Kriptografi Politikalarına ilişkin Yönerge ile ilgili Konsey Tavsiyesi [C(97)62/FİNAL]; Kritik Bilgi Altyapılarının Korunmasına ilişkin Yönerge ile ilgili Konsey Tavsiyesi [C(2008)35]; İnternet Ekonomisinin Geleceğine ilişkin Bildirge (Seul Bildirgesi) [C(2008)99]; İnternet Politikaları Oluşturma İlkeleri ile ilgili Konsey Tavsiyesi [C(2011)154]; Düzenleyici Politikalar ve Yönetim ile ilgili Konsey Tavsiyesi [C(2012)37]; Dijital Devlet Yönetimi Stratejileri ile ilgili Konsey Tavsiyesi [C(2014)88]; ve Kritik Risklerin Yönetimi ile ilgili Konsey Tavsiyesi [C/MIN(2014)8/FİNAL] **UYARINCA;**

Bu Tavsiye Metninin yerine geçtiği Bilgi Sistemlerinin Güvenliğine ilişkin OECD Rehber İlkeleri – Güvenlik Kültürüne Doğru ile ilgili Konsey Tavsiyesi [C(2002)131/FİNAL] **UYARINCA;**

İnternet de dahil olmak üzere dijital ortamın ekonomilerimizin ve toplumlarımızın işleyişi için oldukça önemli olduğunu ve büyümeyi, yenilikçiliği, refahı ve kapsayıcılığı canlandırdığını **GÖZ ÖNÜNE ALARAK**;

Dijital ortamın sunduğu faydaların ekonominin tüm sektörlerine ve sosyal gelişimin her yönüne nüfuz ettiğini; bu faydaların bilgi teknolojilerinin ve altyapısının, özellikle de İnternetin küresel, açık, birbiri ile bağlantılı ve dinamik doğasından kaynaklandığını **GÖZ ÖNÜNE ALARAK**;

Dijital ortamın kullanımı, yönetimi ve geliştirilmesinin dinamik yapılı belirsizliklere dayandığını **GÖZ ÖNÜNE ALARAK**;

Dijital güvenlik risk yönetiminin bu belirsizliklere hitap etmek ve beklenen sosyal ve ekonomik faydalardan tam anlamıyla yararlanmak, temel hizmetleri sunmak ve kritik altyapıları işletmek, insan haklarını ve temel değerleri korumak ve bireyleri dijital güvenlik tehditlerden korumak adına esnek ve çevik bir yaklaşım teşkil ettiğini **GÖZ ÖNÜNE ALARAK**;

Dijital güvenlik risk yönetiminin OECD Güvenlik Esas İlkelerinde bulunan "Güvenlik Tedbirleri İlkesi"nin uygulanmasında sağlam bir temel oluşturduğunu ve daha da genel olarak bu Tavsiye Metninin ve OECD Güvenlik Esas İlkelerinin birbirlerini güçlendirdiğini **VURGULAYARAK;**

Devletlerin, kamu ve özel sektör kurumlarının yanında bireylerin de kendi rolleri ve bağlamları uyarınca dijital güvenlik risk yönetiminde ve dijital ortamın korunmasında sorumlulukları paylaştıklarını ve yerel, bölgesel ve uluslararası düzeyde işbirliğinin kilit öneme sahip olduğunu da **DİKKATE ALARAK;**

Dijital Ekonomi Politikaları Komitesinin teklifi üzerine KONSEY:

I. Bu Tavsiye Metnine taraf olan üye ve üye olmayan ülkelerin (bundan sonra "Taraflar" olarak anılacaktır)
1. Bölüm 1'de ortaya konulan ilkelerin (bundan sonra "İlkeler" olarak anılacaktır) her düzeydeki tüm devlet ve kamu kuruluşlarında uygulamaya geçirmelerini;
2. Bölüm 2'de ortaya konulduğu şekilde dijital güvenlik risk yönetiminde ulusal bir strateji benimsemelerini
ÖNERMEKTEDİR

II. Hükümetlerde ve kamu ve özel sektör kurumlarındaki en yüksek düzeydeki yöneticilere güven oluşturmak adına dijital güvenlik risk yönetimi yaklaşımını benimsemeleri ve açık dijital ortamın olanaklarından ekonomik ve sosyal refah için yararlanmaları
ÇAĞRISINDA BULUNMAKTADIR

III. Özel kuruluşların dijital güvenlik risk yönetimi yaklaşımlarında İlkeleri benimsemelerini
TEŞVİK ETMEKTEDİR

IV. Tüm paydaşların kendi karar alma süreçlerinde, üstlendikleri rollere, yetkinliklerine ve bağlama göre İlkeleri uygulamasını
TEŞVİK ETMEKTEDİR

V. Hükümetlere ve kamu ve özel sektör kurumlarına, işbirliği içinde dijital güvenlik risk yönetimi adına bireyleri ve küçük ve orta ölçekli işletmeleri güçlendirmek üzere
ÇAĞRIDA BULUNMAKTADIR

VI. İlkelerin birbirini tamamlayıcı nitelikte olduğunu ve bir bütün olarak ele alınmaları gerektiğini ve aynı zamanda risk yönetimi süreçleri, en iyi uygulamalar, metodolojiler ve standartlarla tutarlı bir yapıları olduğunu
KABUL ETMEKTEDİR

VII. Bunlara ek olarak; bu Tavsiye Metni bağlamında, aşağıdaki maddeleri **KABUL ETMEKTEDİR**:

1. Risk, belirsizliklerin hedefler üzerindeki etkileri olarak tanımlanmaktadır. "Dijital Güvenlik Riski", herhangi bir faaliyetteki dijital ortamın kullanımı, geliştirilmesi ve yönetimi ile ilgili risk kategorisini tanımlamak için kullanılmaktadır. Bu risk dijital ortamdaki tehditlerin ve açıkların bileşimi neticesinde ortaya çıkabilir. Bu risk, ilgili faaliyet ya da ortamın gizliliğini, bütünlüğünü ve bulunabilirliğini bozarak ekonomik ve sosyal hedeflerin gerçekleştirilmesini sekteye uğratabilir. Dijital güvenlik riski doğası gereği dinamik bir yapıdadır. Dijital ve fiziksel ortamlar, faaliyetle ilgili bireyler ve faaliyeti destekleyen organizasyon süreçleri ile ilgili bileşenleri barındırır.

2. "Dijital güvenlik risk yönetimi", belli bir kurum dahilinde ve/veya kurumlar arasında dijital güvenlik riskine karşı alınan, aynı zamanda olanakları maksimize eden bir dizi eşgüdümlü eylemdir. Hem karar alma sürecinin, hem de ekonomik ve sosyal faaliyetlerdeki genel risk yönetimi çerçevesinin bir parçasıdır. Bütünsel, sistematik ve esnek bir dizi döngüsel ve aynı zamanda olabildiğince şeffaf ve açık olan süreçlere dayanmaktadır. Bu süreçler dizisi, dijital güvenlik risk yönetimi önlemlerinin ("güvenlik önlemleri") ilgili risk ve ekonomik ve sosyal hedeflere göre uygun ve orantılı olmasını sağlamaya yardımcı olur.

3. “Paydaşlar”, ekonomik ve sosyal faaliyetlerinin tamamında ya da bir kısmında dijital ortama gereksinim duyan hükümetler, kamu ve özel sektör kurumları ve bireylerdir. Paydaşlar farklı rollere sahip olabilir. “Liderler ve karar alıcılar” hükümetlerde ve kamu ve özel sektör kurumlarında en üst düzey yönetimde bulunan paydaşlardır.

BÖLÜM 1. İLKELER

Genel İlkeler

1. Farkındalık, beceriler ve güçlendirme

Tüm paydaşlar dijital güvenlik riskini ve nasıl yönetileceğini anlamalıdır.
Paydaşlar dijital güvenlik riskinin ekonomik ve sosyal hedeflerin yerine getirilmesini etkileyebildiğinin ve dijital risk yönetimlerinin diğerlerini etkileyebildiğinin farkında olmalıdır. Bu riski anlayıp yönetebilmeye yardımcı olmak ve dijital güvenlik risk yönetimlerinin kendi faaliyetlerine ve tüm dijital ortama olan potansiyel etkilerini değerlendirebilmek adına gerekli eğitim ve becerilerle güçlendirilmelidirler.

2. Sorumluluk

Tüm paydaşlar dijital güvenlik risk yönetimi için sorumluluk üstlenmelidir.
Paydaşlar, üstlendikleri roller, bağlam ve hareket kabiliyetleri uyarınca dijital güvenlik risk yönetiminde ve kararlarının diğerleri üzerindeki potansiyel etkilerini dikkate alma açısından sorumlu davranmalı ve hesap verebilir durumda olmalıdır. Ekonomik ve sosyal hedefleri gerçekleştirebilmek için belli bir seviyede dijital güvenlik riskinin kabul edilebilir olacağını dikkate almaları gerekmektedir.

3. İnsan hakları ve temel değerler

Tüm paydaşlar dijital güvenlik risk yönetimini şeffaf bir şekilde ve insan hakları ve temel değerler ile tutarlı bir düzlemde yürütmelidir.
Dijital güvenlik risk yönetimi demokratik toplumların kabul ettiği ifade özgürlüğü, bilginin serbest dolaşımı, bilginin ve iletişimin mahremiyeti, gizliliğin ve kişisel verilerin korunması, açıklık ve adil yargılama gibi insan hakları ve temel değerler ile uyumlu olacak bir şekilde uygulanmalıdır. Dijital güvenlik risk yönetimi başkalarının ve bir bütün olarak toplumun yasal çıkarlarını tanıyan ve buna riayet eden bir etik davranışa dayandırılmalıdır. Kurumlar dijital güvenlik risk yönetimlerindeki uygulamaları ve yöntemleri hususunda genel bir şeffaflık politikası izlemelidir.

4. İşbirliği

Tüm paydaşlar sınır ötesi de dahil olmak üzere işbirliği içinde olmalıdır.
Küresel bağlantı paydaşlar arasında birbirine bağlılık oluşturur ve dijital güvenlik risk yönetimi adına birbirleri ile işbirliği içinde olmalarını sağlar. İşbirliği tüm paydaşları içermelidir. İşbirliği devlet yönetimi ile kamu ve özel sektör kurumlarının bünyelerinde olmasının yanında birbirleriyle ve bireylerle de olmalıdır. İşbirliği aynı zamanda bölgesel ve uluslararası olarak sınır ötesine de taşınmalıdır.

Uygulama İlkeleri

5. Risk değerlendirmesi ve müdahale döngüsü

Liderler ve karar alıcılar dijital güvenlik riskinin devamlı risk değerlendirme temelinde ele alınmasını sağlamalıdırlar.
Dijital güvenlik risk değerlendirmesi sürekli olarak devam eden sistematik ve döngüsel bir süreç ile yerine getirilmelidir. Tehditlerin potansiyel sonuçlarının yanında tehlike içindeki ekonomik ve sosyal faaliyetlerin zayıflıklarını da değerlendirme içine almalı ve karar alma sürecini riske müdahale için haberdar etmelidir. Riske müdahale, ilgili faaliyetlerden beklenen ekonomik ve sosyal faydalara oranla riski kabul edilebilir bir seviyeye indirmekle beraber, başkalarının yasal çıkarlarına olan potansiyel etkisini de dikkate almalıdır. Risk müdahalesi farklı seçenekleri ya da bunların herhangi bir bileşimini içerir: riski kabul etmek, azaltmak, aktarmak, riskten kaçınmak.

6. Güvenlik önlemleri

Liderler ve karar alıcılar güvenlik önlemlerinin risk için uygunluğunu ve orantılılığını sağlamalıdır.
Dijital güvenlik risk değerlendirmesi, dijital güvenlik riskinin risk değerlendirme ve müdahale sürecinde belirlenen kabul edilebilir seviyelere indirmek adına güvenlik önlemlerinin seçilmesi, uygulanması ve iyileştirilmesi süreçlerini yönlendirmelidir. Güvenlik önlemleri riske uygun ve orantılı olmalı ve önlemlerin seçimi esnasında korunması amaçlanan ekonomik ve sosyal faaliyetler üzerinde, insan hakları ve temel değerler üzerinde ve başkalarının yasal çıkarları üzerinde olabilecek potansiyel olumlu ya da olumsuz etkileri dikkate alınmalıdır. Fiziksel, dijital ya da faaliyet ile ilişkili insanlar, süreçler ya da teknolojiler ile ilgili olsun, her türlü önlem dikkate alınmalıdır. Kurumlar olası zayıflıkları mümkün olan en kısa zamanda ortaya çıkarmalı ve bunlara müdahale etmelidir.

7. İnovasyon

Liderler ve karar alıcılar inovasyonun dikkate alınmasını sağlamalıdır.
İnovasyon dijital güvenlik riskinin, risk değerlendirmesi ve müdahale sürecinde belirlenen kabul edilebilir seviyeye düşürülmesinin bir parçası olarak ele alınmalıdır. Dijital ortama dayanan ekonomik ve sosyal faaliyetlerin tasarım ve uygulama aşamasının yanında güvenlik önlemlerinin tasarım ve geliştirme aşamalarında da inovasyon teşvik edilmelidir.

8. Hazırlık ve süreklilik

Liderler ve karar alıcılar hazırlık ve devamlılık planlarının benimsenmesini sağlamalıdır.
Güvenlik vakalarının olumsuz etkilerini azaltabilmek ve ekonomik ve sosyal faaliyetlerin devamlılığını ve dirençliliğini desteklemek adına, dijital güvenlik risk değerlendirmesi baz alınarak bir hazırlık ve devamlılık planı yapılmalıdır. Bu plan, dijital güvenlik vakalarında önlem, tespit, müdahale ve kurtarma işlemleri için gerekli olan tedbirleri belirlemelidir. Plan, dijital güvenlik vakalarının büyüklüğü ve ağırlığının yanında dijital ortamdaki başkalarına etkilerini de dikkate alan açık yükselme seviyeleri isnat edecek mekanizmalar sağlamalıdır. Uygun bildirim prosedürleri planın uygulanmasının bir parçası olarak düşünülmelidir.

BÖLÜM 2. ULUSAL STRATEJİLER

A. Dijital güvenlik risk yönetimi için oluşturulan ulusal stratejiler İlkeler ile uyum içinde olmalı ve tüm paydaşların ekonomik ve sosyal faaliyetler için dijital güvenlik risk yönetiminde bulunabilmelerini sağlamanın yanında dijital ortamda güven ve mahremiyeti teşvik edici olmalıdır. Bu stratejiler:

1. En üst seviye devlet yetkililerince desteklenmeli ve esnek, teknolojiden bağımsız ve ekonomik ve sosyal refahı teşvik edici diğer stratejilerle uyum içinde olan, açık ve tüm devlet kurumlarını içeren bir yaklaşımı ifade etmelidir.

2. Ekonomik ve sosyal refah için sınırlar dahilinde ve sınırlar arasında teknoloji, iletişim ve verilerin akışını engellemeyecek şekilde, toplam dijital güvenlik risk seviyesini düşürmek adına açık dijital ortamdan faydalanmayı hedeflediğini açıkça ifade etmeli; bireyleri dijital güvenlik tehditlerinden korumanın yanında ulusal ve uluslararası güvenliği de sağlamak ve insan hakları ve temel değerleri korumak adına temel hizmetlerin sunulması ve kritik altyapıların işletilmesini sağlamayı hedeflemelidir.

3. Tüm paydaşlara hitap etmeli; küçük ve orta ölçekli işletmelere ve bireylere uygun olacak şekilde düzenlenmeli; ve paydaşların üstlendikleri rollere, iş yapma yetilerine ve iş yaptıkları bağlama göre sorumluluklarının ve hesap verebilirliklerinin üzerinde durmalıdır.

4. Devlet içi işbirliği yaklaşımı ve tüm paydaşların dahil olduğu açık ve şeffaf bir süreç sonucu ortaya çıkmalı ve düzenli olarak deneyim ve en iyi yöntemlere dayanmalı, ve gerektiğinde uluslararası karşılaştırılabilir ölçütler kullanılmalıdır.

B. Ulusal stratejiler hükümetlerin aşağıdaki ilkeler ışığında hareket edeceği tavırları içermelidir:

1. Özellikle aşağıdaki maddeleri uygulamak suretiyle, Örnek oluşturarak liderlik etmek:

i). Devletin kendi faaliyetlerinde dijital güvenlik risk yönetimi için bütüncül bir çerçeve yapı benimsemek. Çerçeve yapı ve uygulama politikaları, devlet faaliyetleri ve davranışlarında, tespit edilen dijital güvenlik açıklarının ve ilgili azaltma önlemlerinin de açıklanması dahil olmak üzere güven ve mahremiyeti tesis etmek adına şeffaf olmalıdır;

ii). Tüm ilgili devlet aktörleri arasında, dijital risk yönetimlerinin uyumlu olması ve ekonomik ve sosyal refahı iyileştirebilmesi adına işbirliği mekanizmaları oluşturmak;

iii). Ulusal düzeyde bir veya daha fazla Bilgisayar Acil Müdahale Ekibi (BAME) olarak da bilinen Bilgisayar Güvenliği Vakası Müdahale Ekibi (BGVME) oluşturulmasını ve devlete bağlı ya da özel BGVMElerin sınır ötesi de dahil olmak üzere işbirliği içinde çalışmalarının teşvikini sağlamak;

iv). Kamu ihalesi politikaları ve uygun risk yönetimi özelliklerine sahip uzmanların istihdamı da dahil olmak üzere kendi piyasa konumlarını dijital güvenlik risk yönetimini tüm ekonomide ve toplumda teşvik etmek üzere kullanmak;

v). Dijital güvenlik risk yönetiminde uluslararası standartların ve en uygun yöntemlerin kullanılmasını teşvik etmek ve açık, şeffaf ve çoklu paydaşlı süreçler ile bunların geliştirilmesi ve gözden geçirilmesine ön ayak olmak;

vi). Bilginin durağan ve hareketli olduğu durumlarda uygun bir biçimde korunmasını sağlamak adına dijital güvenlik risk yönetiminde yenilikçi teknikler benimsemek ve veri toplama ve saklamada uygun sınırlamaların da faydalarını dikkate almak;

vii).İnovasyonu da teşvik edecek şekilde dijital güvenlik risk yönetiminde kamu araştırmalarını ve geliştirmelerini koordine etmek ve desteklemek;

viii). Özellikle dijital güvenlik risk yönetimine daha geniş beceri stratejisiyle yaklaşarak dijital güvenlik risk yönetiminde rol alacak nitelikli işgücünün geliştirilmesini desteklemek. Bu, hizmet içi risk yönetimi eğitim ve sertifika programlarını ve özellikle yükseköğretimde ulusal düzeyde tüm nüfus üzerinde dijital becerileri geliştirecek eğitim programlarını desteklemeyi kapsayacak şekilde yapılabilir;

ix). Bilişim suçlarını azaltmaya yardımcı olmak adına halihazırdaki uluslararası araçları kullanarak bütüncül bir çerçeve yapı benimsemek;

x). İlgili stratejileri uygulayabilmek için gerekli kaynakları tahsis etmek.

2. Özellikle aşağıdaki maddeleri uygulamak suretiyle, Uluslararası işbirliği ve karşılıklı yardımı güçlendirmek:

i). İlgili bölgesel ve uluslararası forumlara katılmak ve iki ya da daha fazla taraflı ilişkiler oluşturup deneyimleri ve en iyi uygulamaları paylaşmak ve diğer ülkelerin risk faktörünü arttırmayacak ulusal dijital güvenlik risk yönetimi yaklaşımını desteklemek;

ii). Uygun bir gönüllülük esasınca diğer ülkelere yardım ve destek sunmak ve dijital güvenlik risk yönetimi meseleleri ile ilgili sınır ötesi taleplere zamanında karşılık verebilmek adına ulusal iletişim noktaları oluşturmak;

iii). BGVMElerin işbirliği, koordineli tatbikatları ve benzeri diğer işbirliği araçlarını da kullanarak ülke içinde ve sınır ötesindeki tehditlere müdahalenin iyileştirilmesi için çalışmak.

3. Özellikle aşağıdaki maddeleri uygulamak suretiyle, Diğer paydaşlar ile ilişki içinde olmak:

i). Faaliyetlerinde dijital güvenlik risk yönetimini daha iyi yerine getirebilmeleri için devletlerin ve diğer paydaşların birbirlerine nasıl yardım edebileceklerini araştırmak;

ii). Devlet politikalarının diğer paydaşların faaliyetlerine ya da ulusal ekonomik ve sosyal refaha olabilecek potansiyel olumsuz etkilerini belirleyip bunlara müdahale etmek;

iii). Dijital güvenlik risk yönetimini halka duyurmak için uygulamalar ve prosedürler oluşturmak;

iv). Tüm paydaşlar tarafından dijital güvenlik açıklarının sorumlu bir şekilde ortaya çıkarılması, bildirilmesi ve/veya düzeltilmesini teşvik etmek;

v). Dijital güvenlik risk yönetimi için, farklı kategorilerdeki paydaşların gereksinimlerine göre tasarlanmış teknolojiden bağımsız girişimler vasıtalarıyla toplumun tüm katmanlarına farkındalık, beceri ve yetki seviyesini arttırmak.

4. Özellikle aşağıdaki maddeleri uygulamak suretiyle, Tüm paydaşların dijital güvenlik risk yönetiminde işbirliği yapabilmeleri için gerekli koşulları oluşturmak:

i). Aşağıda sıralanmış maddeleri yerine getirebilmek adına kamu-özel, resmi ya da gayri resmi, yerel, bölgesel ya da uluslararası seviyelerde, karşılıklı güven üzerine kurulmuş girişimlere ve ortaklıklara ilgili paydaşların aktif katılımını teşvik etmek:
– Politika ve uygulama seviyelerinde, dijital güvenlik risk yönetimine dair bilgi, beceri ve başarılı deneyim ve uygulamaların paylaşımında bulunmak;
– Dijital güvenlik risk yönetimine dair bilgi alışverişinde bulunmak;
– Gelecek zorluklar ve fırsatlar için beklenti ve planlar oluşturmak.

ii). Dijital güvenlik riskinin azaltılmasının yanında açıkların ve tehditlerin ortaya çıkarılması ve iyileştirilmesi hususunda paydaşlar arasında koordinasyonu teşvik etmek;

iii). Bireyleri ve küçük ve orta ölçekli işletmeleri dijital güvenlik tehditlerine karşı korumak ve ekonomik ve sosyal faaliyetlerinde dijital güvenlik risk yönetim becerilerini artırmak için tüm paydaşların birlikte çalışmalarına teşvik etmek;

iv). Paydaşların dijital güvenlik risk yönetimi, piyasa şeffaflığı ve verimliliğine yönelik uygun teşvikler sağlamak;

v). Bireylerin ve kurumların dijital ortamdaki faaliyetleri korumak için kullanabilecekleri araçların geliştirilmesinin yanında dijital güvenlik risk yönetiminde inovasyonu da teşvik etmek;

vi). Dijital güvenlik risk yönetiminin etkinliğini, verimliliğini ve şeffaflığını arttırmak için uygun bir biçimde genel geçer ölçüm metodolojilerine, standartlarına ve en iyi uygulamalara dayalı uluslararası karşılaştırılabilir risk ölçütlerinin geliştirilmesini teşvik etmek.

VIII. Tavsiye Metnini uygulamaya geçirmek, kamu ve özel sektörde, Taraf olmayanlara ve uluslararası forumlara duyurmak ve yaymak üzere Tarafların işbirliğinde olmasını **TAVSİYE ETMEKTEDİR.**

IX. Üye olmayan ülkeleri bu Tavsiye Metnine taraf olmak üzere **DAVET ETMEKTEDİR.**

X. Dijital Ekonomi Politikaları Komitesini, Tavsiyelerin kabul edilişinden itibaren üç yıl içinde ve daha sonra da uygun aralıklarla olmak üzere uygulama durumunu denetlemek ve Konseye raporlamak üzere **GÖREVLENDİRMEKTEDİR**.

Ekonomik ve Sosyal Refah için Dijital Güvenlik Risk Yönetimi OECD Tavsiye Metni için Yardımcı El Kitabı

Yardımcı El Kitabı açıklayıcı ve örneklendirici niteliktedir. Ekonomik ve Sosyal Refah için Dijital Güvenlik Risk Yönetimi Konsey Tavsiye Metninin bir parçası değildir.

İçindekiler

Giriş

Geçtiğimiz on yıl içinde, Bilgi ve İletişim Teknolojileri (BİTler), İnternet de dahil olmak üzere ekonominin işleyişinde oldukça önem kazanmış ve tüm sektörlerdeki kalkınmanın ana itici gücü olmuştur. Hükümetler, kamu ve özel sektör kurumlarının yanında bireyler de artık temel faaliyetleri için dijital ortama bağlı hale gelmiştir. Bununla birlikte dijital ortamın kullanımıyla birlikte ortaya çıkan artan sayıdaki belirsizliklerle de yüzleşmek durumunda kalmışlardır. Dijital güvenlik tehditleri ve vakalarının sayısı artmış, bu da finansal, gizlilik ve itibar açısından, hatta bazı durumlarda fiziksel zararlara bile yol açabilen sonuçlara neden olmuştur. Her ne kadar paydaşlar giderek dijital güvenlik risklerinden kaynaklanan güçlüklerin daha fazla farkında olsalar da duruma genelde teknik açıdan yaklaşmakta, ekonomik ve sosyal karar alma yönünü hesaba katmamaktadırlar. Dijital güvenlik risk yönetiminin her şeyden önce ekonomik ve sosyal karar almanın bir parçası olduğunu anlatmak paydaşların dijital ortamın getirdiği fırsatlardan tam anlamıyla yararlanmalarını sağlamak adına zorunlu hale gelmiştir.

Dijital güvenlik meseleleri genellikle kullanışlı ve kapsayıcı bir terim olan ve teknolojiden tutun ekonomik ve sosyal, hukuk, adli, insan hakları, ulusal güvenlik, savaş, uluslararası istikrar, istihbarat gibi tüm yönleriyle dijital güvenliği kapsayan "siber güvenlik" terimi ile ifade edilmektedir. Bu terimin yaygın kullanımı söz konusu meselenin geniş ve karmaşık yapısını gölgelemektedir. Dijital güvenlik, her biri farklı kültür ve arka plandan, kabul edilmiş uygulamalardan ve hedeflerden kaynaklanan en az dört farklı perspektiften yaklaşılabilir:

- *Teknoloji,*dijital ortamın işleyişi üzerine odaklıdır (uzmanları tarafından genellikle "bilgi güvenliği", "bilgisayar güvenliği" ya da "ağ güvenliği" olarak adlandırılmaktadır)
- *Emniyet,*ve genel olarak hukuki yönler (örneğin siber suçlar)
- *Ulusal ve uluslararası güvenlik*, BİTlerin istihbarat, çatışma önleme, savaş vs. gibi durumlardaki rolleri de buna dahildir.
- *Ekonomik ve sosyal refah*, dijital ortamın gelişiminde öncülük ettiği ekonomideki tüm sektörlerde[1] refah, inovasyon, rekabetçilik ve istihdamın yanında bireysel özgürlükler, sağlık[2], eğitim[3], kültür, demokratik katılım, bilim, eğlence, ve diğer refah etkenleri.

"Daha iyi yaşam için daha iyi politikalar" düsturu ile uyumlu olarak OECD dijital güvenlik riskine ekonomik ve sosyal perspektiften yaklaşmaktadır.

OECD Konseyi[4] 2015 yılında dijital ekonomi politikaları için[5] geniş bir çerçevedeki Tavsiyeler, rehberlik ve analitik çalışmalarının parçası olarak *Ekonomik ve Sosyal Refah için Dijital Güvenlik Risk Yönetimi Konsey Tavsiye Metnini* ("Tavsiye Metni") benimsemiştir. İki yılı aşkın bir sürenin ürünü olan Tavsiye Metni, OECD'nin 1980 yılındaki *Gizliliğin Korunması ve Kişisel Verilerin Sınırlar arası Akışına İlişkin Yönerge ile ilgili Konsey Tavsiyesi* (2013'te değiştirilen "Gizlilik Ana İlkeleri")(OECD, 2013b) ile başlayan, kriptografi politikaları, elektronik doğrulama ve kritik bilgi altyapılarının korunması (OECD, 2008) gibi diğer önemli yasal belgelerle devam eden, otuz yılı aşkın dijital ekonomide güven ve inovasyon için politika ve araç geliştirme deneyimi üzerine bina edilmiştir. Tavsiye Metni,1992 *Bilişim Sistemlerinin Güvenliğine dair Ana Esaslar için Konsey Tavsiyeleri*nin ("ilk Güvenlik Ana Esasları") yerine kabul edilen *2002 Bilişim Sistemleri ve Ağlarının Güvenliğine dair Ana Esaslar için Konsey Tavsiyeleri: Güvenlik Kültürüne Doğru* ("Güvenlik

Ana Esasları") (OECD, 2008) metninin yerine geçmektedir. Bu nedenle, Tavsiye Metni, dijital ekonominin ve özellikle tüm ekonomik sektörlerin ve sosyal yaşantının başarılı bir şekilde işleyişi ve gelişiminde sahip olduğu temel rolün evrimini yansıtan olgunlaşma sürecinin üçüncü büyük kilometre taşıdır.

Metindeki tüm Tavsiyeler yasal bağlayıcılığı olmayan Kurum Kararları olup, Üye ülkelerin siyasi iradesini yansıtmalarından dolayı uygulanmaları halinde manevi güç nitelikleri bulunmaktadır. Üye ve üye olmayan ülkelerin ("Taraflar"ın), Tavsiyelere taraf olmalarından sonra onları bütünüyle uygulamak için tüm güçleriyle çaba sarf edecekleri beklenmektedir[6]. Bu Tavsiye Metni, devlet politikaları belirleyicileri, iş ve sanayi dünyası, sivil toplum ve teknoloji camiası[7] gibi çok paydaşlı bir sürecin uzlaşısı ve bilgilendirmesiyle oluşturulmuştur. OECD üyeliğinin dışındaki devletler, resmi olarak Tavsiye Metnine taraf olmayı seçseler de seçmeseler de tavsiyeleri kendi ulusal stratejilerini geliştirmekte kullanmaları teşvik edilmektedir. Buna ek olarak, tüm kamu ve özel sektör kurumlarının kendi risk yönetim çerçevelerini oluştururken İlkeleri dikkate almaları teşvik edilmektedir. Diğer uluslararası ve bölgesel kuruluşlar da Tavsiye Metnini kendi işlerine ve faaliyetlerine yansıtmakta serbesttir, hatta bunun için teşvik edilmektedir[8].

Tavsiye Metni, yukarıda bahsedilen farklı boyutların (ekonomik, sosyal, teknik, hukuki, ulusal güvenlik ve uluslararası güvenlik) dijital ortamda, dışında olduğu gibi birbirleri ile bağlantılı olduğunu kabul etmektedir. Bu nedenler hükümetler dijital güvenlik riskinin farklı boyutları için tüm devlet kurumlarını içeren bir yaklaşım için gayret göstermeli ve tutarlık, bütünsellik ve karşılıklı güçlendirmeyi amaçlamalıdır.

Bu bağlamda Tavsiye Metni, rekabet halindeki politika hedeflerini uygun bir dengede tutabilmek adına, hükümetlere en üst yönetim düzeyinde desteklenen (Bölüm 2. A. 1) ulusal dijital güvenlik risk yönetimi stratejilerini benimseme (I. 2) çağrısında bulunmaktadır. Tavsiyelerin uygulanmasının yerel, bölgesel ve uluslararası düzeyde dijital güvenlik meselelerinin farklı boyutlarına hitap eden uzmanların işbirliğinin teşvik etmesi beklenmektedir.

Tavsiye Metninin ve daha genel olarak OECD'nin bu alandaki çalışmalarının, çok sayıda kuruluşu ve onların kendi özel düsturlarını yansıtan çalışmaları barındıran uluslararası bir diyalogun bir parçası olduğunu vurgulamak gerekmektedir. Örneğin, Avrupa Konseyi siber suçlar ile ilgili meselelerle ilgilenmektedir (örneğin 2001 Budapeşte Siber Suçlar Sözleşmesi)[9]; Interpol emniyet güçlerinin işbirliğini sağlamaktadır[10]; Birleşmiş Milletler[11] ve Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT)[12] devletlerin dijital ortamdaki davranışlarını ve uluslararası istikrarı korumak için gerekli güven inşa eden tedbirleri ele almaktadır; teknik standartlar Uluslararası Standartlar Teşkilatı (ISO), İnternet Mühendisliği Görev Gücü (IETF), Dünya Çapında Ağ Birliği (W3C), Yapısal Bilgi Standartları Oluşumu Organizasyonu (OASIS) gibi farklı ortamlarda geliştirilmektedir. Asya Pasifik Ekonomik İşbirliği Örgütü (APEC)[13] gibi bölgesel kuruluşlar da en iyi uygulamaların ve rehber ilkelerin uygulanmasını teşvikinde önemli rol oynamaktadır.

Tavsiye Metni bir girizgah ile başlamakta ("Uyarınca", "Dikkate alarak"... gibi kısımlar), bunu daha sonra Konseyin (buradan itibaren "OECD" olarak kullanılacaktır) devletlere ve paydaşlara olan önerileri ("I. ... Önermektedir", "II. ... Çağrıda Bulunmaktadır" gibi kısımlar) ve bunun yanında İlkeler hakkında bilgileri ("VI. ... Kabul etmektedir" gibi kısımlar) ve terminoloji hakkında açıklamaları ("VII. ... Kabul Etmektedir" gibi kısımlar) numaralandırılmış şekilde sunmaktadır. Bu kısımda OECD hükümetteki ve kamu ve özel

kurumlardaki en üst düzey yetkililere ekonomik ve sosyal refah adına güven tesis eden ve açık dijital ortamdan yararlanan bir dijital güvenlik risk yaklaşımı benimsemeleri çağrısında bulunmaktadır.

Bölüm 1, dijital güvenlik risk yönetimi üzerine sekiz adet birbiriyle ilişkili, birbirine bağlı ve birbirini tamamlayıcı yüksek düzey ilke (buradan sonra "İlkeler" olarak anılmaktadır) ile bütünsel bir çerçeve sunmaktadır. OECD, tüm Tarafların tüm devlet yönetimi seviyelerinde[14] ve kamu kurumlarında bu İlkelerin uygulanmasını tavsiye etmektedir (I. 1). Konsey aynı zamanda ticari ya da kar amacı gütmeyen tüm özel kuruluşların dijital güvenlik risk yönetimlerinde bu İlkeleri benimsemelerini (III) ve kendi üstlendikleri rollere, yetkilerine ve bağlama göre İlkeleri karar alma süreçlerine dahil etmelerini teşvik etmektedir[15] (IV).

Böylelikle İlkeler, doğrudan kamu ve özel sektör kurumlarının kendi kurumsal ve örgütsel risk yönetimi politikalarını geliştirirken rehber olarak kullanılabilir ya da dolaylı olarak ulusal stratejiler ve ilgili kamu politikaları geliştirilmesinde esin kaynağı olabilirler. Özellikle bununla ilgili olarak Tavsiye Metni, Tarafların İlkelerden hareketle ortaya konulmuş ama farklı yapıyla Bölüm 2'de sunulmuş olan rehber esaslara uymak suretiyle dijital güvenlik risk yönetimi için ulusal bir strateji benimsemelerini önermektedir.

Genel bağlamda Tavsiye Metni, kurumlarda uygun bir dijital güvenlik risk yönetimi idare çerçevesi, devlet yönetiminde de ekonomik ve sosyal refaha temas eden bir ulusal strateji benimsenmesine öncülük edebilecek en üst düzey yetkililere ("liderler ve karar alıcılar") hitap etmektedir.

Tavsiye Metninin tasarlanmasının ilk aşamalarından itibaren OECD delegasyonları ilgili konunun karmaşıklığını ve temel bilgileri ve açıklamaları içeren ayrı bir dokümanın geliştirilmesi vasıtasıyla Tavsiye Metninin uygulanabilirliğini sağlamak gerektiğini kabul etmişlerdir. Bunun yanında "Yardımcı El Kitabının" kısa ve dijital güvenlik risk yönetiminin sadece en temel olgularına hitap edecek bir yapıda olması gerektiği ve dolayısıyla sadece Tavsiye Metnindeki Bölüm 1'e odaklanması gerektiği konusunda uzlaşmışlardır. Daha ileride yapılacak olan çalışmalar Yardımcı El Kitabında ortaya konulan bazı hususlara ve daha ayrıntılı yaklaşım sunabilir. Kitapçığın Ek bölümü Yardımcı El Kitabının ortaya koyduğu danışma ve tasarı evrelerinin yanında gelecekte yapılması muhtemel çalışma alanlarının bir listesini sunmaktadır.

El Kitabı, kısa bir bağlam tanımı yaptıktan sonra Tavsiye Metnindeki ana kavramları ele almakta, İlkelerin paydaşlarca uygulanabilirliğini yorumlamakta ve son olarak da sekiz İlkenin her biri için açıklama sunmaktadır.

Bağlam

Kamu ve özel sektör kurumlarındaki çoğu lider ve karar yapıcı, dijital ortamın inovasyon, üretkenlik ve büyüme için öncü rol oynamasının yanında ekonomik ve sosyal refahı tehlikeye sokabilecek belirsizliklerin de kaynağı olabileceğinin farkına varmaktadırlar. Dijital güvenlik vakaları kuruluşlar için, örnek olarak faaliyetlerin sekteye uğraması (örneğin hizmet reddi ya da sabotaj neticesinde), doğrudan mali zarar, hukuki davalar, itibar kaybı, rekabetçilik kaybı (örneğin ticari sırların çalınması gibi vakalar) ve müşterilerin, çalışanların, hissedarların ve ortakların güven kaybı gibi oldukça farklı ekonomik sonuçlar doğurabilmektedir. Her ne kadar genelde istisnai olsa da dijital güvenlik vakalarının sanayi tesislerinin, ulaşım sistemlerinin ve hastanelerin BİT (bilgi ve iletişim teknolojileri) kullanımını da dikkate alındığında can kaybı da dahil olmak üzere fiziksel zarara yol açabilecekleri dikkate alınmalıdır.

Hükümetler de diğer kuruluşlar gibi güvenlik vakalarının potansiyel sonuçları ile karşı karşıyadırlar. Kamu politikalarını oluşturanlar olarak vakaların, yukarıda da bahsedildiği üzere ekonomik ve sosyal alanın da ötesine, ulusal ve uluslararası güvenliğe de uzanan yönleriyle makro düzeydeki sonuçlarından kaygı duymaktadırlar.

Son olarak, bireyler de dijital ortamın kullanımından kaynaklanan birçok faydadan mahrum kalabileceklerinin giderek daha fazla farkında olmaktadırlar. Kişisel verileri kamuya ifşa edildiğinde ya da yetkili olmayan insanların eline geçtiğinde bireyler potansiyel fiziksel, mali ve ahlaki zararlara uğratabilecek mahremiyet ihlalleri ile karşı karşıya gelmektedirler[16]. Kişisel verileri ya da dijital kimlikleri kendi cihazlarından, gizliliği ihlal edilmiş şirketlerden ya da devlet bilgi sistemlerinden çalındığında kimlik hırsızlığına bağlı mali dolandırıcılığın kurbanı haline gelebilirler.

Bu tür vakaların sayısının ve karmaşıklığının artmasının birçok nedeni bulunmaktadır. Bunlardan biri, suç faaliyetlerinin çevrimiçi ortamlara doğru kayması sonucu saldırıların giderek profesyonelleşmesi ve genel dijital güvenlik tehdit düzeyini arttırmasıdır. Ara sıra rastlanılan tekil soyguncudan iyi organize olmuş uluslararası gruplara kadar bilumum suçlular, finansman, bilgi ve kimlik hırsızlığı ve bireylere, şirketlere ve devletlere şantaj yapmak gibi suçları işlemek için oldukça yüksek teknik inovasyon becerileri göstermektedir. Diğer faktörler eylemlerini dijital ortama taşıyan, fiziksel saldırılarla paralel olarak İnternet sitelere de saldırılarda bulunan teröristler ve onların destekçilerini de içermektedir. Her ne kadar çok az vaka kapsamlı olarak belgelenmiş olsa da endüstriyel dijital casusluğun da artışta olduğu söylenmektedir[17]. "Hacktivist" olarak bilinen kimseler (bilgisayar sistemlerini ele geçirmek anlamına gelen "hack" ve aktivist kelimelerinin bileşimi) kendi politik amaçlarının görünürlüğünü arttırmak için seçilmiş hedeflere sürekli saldırılarda bulunmaktadır. Son olarak, birçok devlet istihbarat ve saldırı harekatlarını "siber uzay" olarak adlandırdıkları ortamda yürütmektedir. Güvenlikle ilgili dijital belirsizliklerin ana kaynağının, ergenlerin ("kodcu çocuklar") İnternetten buldukları hazır araçlarla rastgele saldırılarda bulunmalarından ibaret olduğu günler çoktan geride kalmıştır.

Kutu 1. 2007-2014: Büyük ölçekli vaka örnekleri

Bu alanda sağlam ve uluslararası olarak karşılaştırılabilir niceliksel ölçütler geliştirmek zor olsa da (OECD, 2012c), ampirik kanıtlar dijital güvenlik vakalarının katlanarak arttığını ve kamu ve özel sektör kurumları, bireyler ve hükümetler olarak herkesi ilgilendirdiğini göstermektedir. Bunlar aşağıdaki örnekleri kapsamaktadır:

2007 yılında Estonya'ya karşı büyük bir "siber atak" silsilesi parlamentoyu, bakanlıkları, bankaları, gazeteleri ve televizyon yayıncılarını etkilemiştir.

2010 yılında Stuxnet virüsü İran'daki nükleer zenginleştirme tesisindeki yüzlerce santrifüjü fiziksel olarak tahrip etmiştir. 2011 yılında Sony PlayStation Ağı'na sızılmış, 77 milyon hesabın kişisel verileri ifşa edilmiş, bu da şirkete resmi olarak 171 milyon dolar ve hatta bazı tahminlere göre 250 milyon dolara kadar maddi zarara mal olmuştur(Gaudiosi, 2014).

2012 yılında Suudi Aramco petrol şirketinin şirket içi ağına bağlı 30000 sabit sürücüsünün dijital işgalciler tarafından silinmesi üzerine verileri kurtarmak iki hafta sürmüştür.

2013 yılında yığın mesaj (spam) karşıtı bir örgüt olan Spamhaus'a karşı büyük ölçekte bir hizmet engelleme (DoS) saldırısı düzenlenmiştir. Bu saldırı eşi görülmemiş bir şekilde ortalama bir DoS saldırısından üç kat daha büyük olarak saniyede 300 gigabit (Gbs) seviyelerine kadar çıkmış ve tespit edilmiş en büyük hizmet engelleme saldırısından üç kat daha fazla büyük olarak kayıtlara geçmiştir (Leyden, 2013). Aynı yıl, ABDli perakende satış şirketi Target, Noel satış sezonunda satış noktası cihazlarına yönelik karmaşık bir saldırıya maruz kalmıştır. Bu saldırı 20 milyon kredi kartı ve bankamatik kartı numarasının ve 110 milyondan fazla müşteri kaydının çalınmasına yol açmış ve tahminlere göre şirkette 148 milyon dolardan bir milyar dolardan fazla bir aralıkta mali zarar oluşturmuştur (O'Connor, 2014).

2014 yılında Home Depot isimli ABD firması da 56 milyon kredi kartı ve bankamatik kartı bilgisi hırsızlığı ile karşı karşıya kalmıştır. Kore'de bir kişi üç büyük banka tarafından verilmiş 104 milyon kredi kartının kişisel bilgilerini çalmış ve 20 milyon kişiyi (ülke nüfusunun %40'ı) mağdur etmiştir. Düzinelerce üst düzey yönetici bunun sonucunda işinden olmuştur (Choe, 2014; Kim, 2014). Aynı yıl, 76 milyon ABD hane halkı ve yedi milyon küçük işletme ile ilgili hesap verileri ABD bankası JPMorgan Chase'den sızdırılmış ve bunun üzerine banka CEO'su şirketin dijital güvenlik bütçesinin 250 milyon dolardan 500 milyon dolara çıkarılacağını ifade etmiştir (Kitten, 2014). Yine aynı yıl, Sony Pictures Entertainment şirket içi ağına yapılan sızma ile şirket içi e-posta yazışmaları, şirket çalışanlarının ve ortaklarının kişisel verilerinin yanında henüz gösterime girmemiş olan filmler ifşa edilmiştir. Bu vakadan başka büyük ölçekli bir siber casusluk operasyonunun (Dragonfly) başta Avrupa ve ABD olmak üzere ilaç ve muhtemelen enerji sektörlerindeki şirketlere karşı yürütüldüğü tespit edilmiştir (Peters, 2014). Son olarak Almanya'daki bir çelik tesisine yapılan bir dijital sızma "büyük ölçekli fiziksel hasara" yol açmıştır (Lee, Assante and Conway, 2014).

Tehdit kaynaklarının profesyonelleşmesi saldırılarda kullanılan teknik araçların, bazıları otomatik hale getirilmiş ve maksimum etki için büyük ölçüde yayılmış, bazıları da tespit ve kaynağının belli edilmesini engellemek için değerli hedeflere özel olarak şekillendirilmiş olmak üzere daha karmaşık hale gelmesine yol açmıştır. Bir yeraltı siber suçlar ekonomisi ortaya çıkmıştır. "Sıfır gün istismarı" (zero-day exploit) olarak adlandırılan, çoğu tarama yazılımından geçebilen zararlı kodlar dijital pazarda satılmaktadır. Bunlar bilgi sistemlerine gizlice girmek, onları uzun süreyle kontrol etmek ve ticari ve politik sırlar gibi gizli verileri almak (buna "İleri Düzey Sürekli Tehdit" (APT) denmektedir) üzere kullanılmaktadır[18]. Sayıları binlerden milyonlara kadar varan virüslü bilgisayarlardan ve cihazlardan oluşan Botnetler[19] (robot ağlar) şantaj ya da hoşnutsuzluk ifadesi için hizmet engelleme saldırılarında bulunmak üzere kiralanabilmektedir. Sosyal mühendislik yöntemleri de oldukça yaygındır; örneğin orijinal gibi görünen e-postalarla saldırganın kimlik bilgilerini çalması ya da kullanıcının sistemine girmesi mümkün olmaktadır (buna "phishing" (oltalama) adı verilmektedir). Kutu 1, karşı karşıya olunan bu güçlüğün kapsamı ve büyüklüğü hakkında farkındalığı arttıran büyük ölçekli vaka örneklerini sunmaktadır.

2009 yılından itibaren dijital güvenlikte karşılaşılan güçlükler OECD ülkelerinde ulusal kamu politikalarında giderek öncelikli bir hal almıştır. Birçok hükümet, en üst siyasi düzeyde destekle "ulusal siber güvenlik stratejileri" benimsemeye başlamıştır. Bu stratejiler bütüncül bir kamu politikası yaklaşımını ve hem devlet yönetimi içinde hem de sivil toplum paydaşlarında yeni işbirliği mekanizmaları kurulmasını teşvik etmiştir[20].

Kamu ve özel sektör kurumları giderek daha fazla bir şekilde[21] karşı karşıya olunan tehlikenin büyüklüğünün farkına varmakta ve uygulamalarını buna göre ayarlamaktadırlar. Özellikle artan sayıda büyük firmalardaki üst düzey yöneticiler salt teknik bir yaklaşımın dijital güvenlik risk yönetiminde yetersiz kaldığını idrak etmektedir. Ancak çoğu kamu ve özel sektör kurumu ve özellikle küçük ve orta ölçekli işletmeler (KOBİler) henüz dijital güvenlik risk yönetimini ekonomik açıdan ele almaya hazır olmamakla birlikte bu meseleye hala genel olarak teknik açıdan bakmaktadırlar. Son olarak kişisel verilerin ifşasına ve bazı vakalarda mali dolandırıcılık ve kimlik hırsızlığına varan sonuçlara neden olan ve sayısı giderek artan büyük ölçekli veri sızmalar, genelde verimli bir şekilde risk yönetimini yürütecek araç, bilgi ve beceriden yoksun olan ve genelde tek başlarına bırakılan bireyleri de kaygılandırmaktadır[22].

Kutu 2. "Bilişim sistemleri güvenliği"nden "dijital güvenlik risk yönetimi"ne (2002-2015)

2015 Tavsiye Metni 2002 Güvenlik Ana Esaslarının devamı niteliğinde olup, aynı zamanda ondan önemli ölçüde farklılıklar barındırmaktadır.

Her iki Tavsiye Metni aynı analizden yola çıkmaktadır: i) dijital ortamın küresel, birbirine bağlantılı, açık ve dinamik yapısı ekonomik ve sosyal refaha öncülük etmekte önemli rol oynamaktadır; ve ii) dijital açıklığı, birbirine bağlantılılığı, ve dinamizmi kaldırmadan ve bu olguların ortaya koyduğu ekonomik ve sosyal faydalardan vazgeçmeden riskin tamamen önlendiği "güvenli ve emin" bir dijital ortamı oluşturmanın imkansızdır. Yani, her iki Tavsiye Metni de İnternet öncesi statik ve katı "çevre güvenliği"nin terkedilmesini ve onun yerine döngüsel ve esnek risk tabanlı bir yaklaşımla risk yönetiminin yürütülmesinin benimsenmesi konusunda uzlaşmaktadır. Bu da riskin bağlama ve ilgili hedefe göre kabul edilir bir seviyeye indirilmesi anlamına gelmektedir.

En büyük değişiklik, İlkelerin odağının "bilişim sistemleri ve ağlarının güvenliği"nden dijital ortama bağımlı ekonomik ve sosyal faaliyetlerdeki güvenlik riskine kaymış olmasıdır. Tavsiye Metni bir faaliyeti yürütmede en üst düzey sorumluluk sahibi olan liderlerin ve karar alıcıların ilgili faaliyette kabul edilebilir risk seviyesini belirlemede ve dijital güvenlik önlemlerinin riske en uygun şekilde olduğunu ve korumayı amaçladıkları faaliyeti engellemediğini sağlamada en uygun kişiler olduğunu kabul etmektedir. Yine de, Tavsiye Metni dijital ortamın tasarımı ve bakımında görevli olan ve dijital güvenlik risk faktörlerini ve ilgili olası güvenlik önlemlerini daha iyi anlayan uzmanlarla (BİT uzmanları) işbirliğinin gerekliliğinin altını çizmektedir.

Buna uygun olarak, riskle ilgili kullanılan dile açıklık getirilmiştir. Tasarı aşamasında "güvenlik" sözcüğünün sözlük karşılığı olan "zarardan ya da tehlikeden azade olma hali" ifadesinin risk yönetimi kavramıyla doğal olarak çelişkide olan ikili ve durağan bir hedef teşkil ettiği konusu dikkate alınmıştır. Hedef kitlenin bir kısmı için "güvenlik" sözcüğü "ulusal güvenlik" ile ilgili kabul edilmekte olup, bu alan doğru ya da yanlış genellikle "güvenlik" kavramının başka her şeyden daha öncelikli olduğu bir kültür ile ilintilidir. Bu nedenle, 2002 Güvenlik Ana Esaslarının aksine Tavsiye Metni "güvenlik" sözcüğünü kendi başına bir hedefi niteleyen isim olarak kullanmak yerine riski, risk faktörlerini ve risk yönetim yaklaşımlarını tanımlayan bir sıfat olarak kullanmaktadır. Aynı şekilde Tavsiye Metni farklı kitleler tarafından farklı anlaşılabileceği ve bunun da karışıklığa yol açabileceği nedeniyle "siber güvenlik" terimini ve "siber" ön ekini ("siber uzay" örneğinde kullanıldığı gibi) kullanmamaktadır. Bunun yanında bu terimler dijital güvenlik riskinin diğer risk kategorilerinden bir şekilde farklı olduğu gibi yanlış bir izlenime yol açabilmektedirler.

Ana Kavramlar

Bu bölüm, Tavsiye Metninde kullanılan ana kavramları açıklamaktadır.

Paydaşlar ve üstlendikleri roller

Tavsiye Metninde kullanıldığı üzere "paydaşlar", "sosyal ve ekonomik faaliyetlerinin tamamı ya da bir kısmı için dijital ortama ihtiyaç duyan hükümetler, kamu ve özel sektör kurumları ve bireyler olup farklı rollere sahip olabilirler" şeklinde ele alınmaktadır (bkz. VII. 3).

Bu terim, farklı seviyelerde, hedeflerini yerine getirebilmek adına ekonomik ve/veya sosyal faaliyetler gerçekleştirmek üzere dijital ortama ihtiyaç duyan tüm oluşumları kapsamayı hedeflemektedir. Hukukiden ziyade sosyolojik olan bu kavram, dijital ortamın doğrudan ve/veya dolaylı olarak kullanılışını belirtmektedir. "Hükümet" terimi her seviyedeki devlet yönetimi organlarını kapsamaktadır (örneğin, merkezi/federal, uluslararası/bölgesel/ulusal/eyalet/yerel vs.). "Kamu kurumları" vergilerle finanse edilen diğer idari birimler gibi kamu ya da idari hukuka tabi olan diğer devlet oluşumları (örneğin hastaneler, okullar, halk kütüphaneleri, vs.) ve kamuya ait işletmelere işaret etmektedir. "Özel kurumlar" özel hukuka tabi olup işletmelerin yanında kar amacı gütmeyen kuruluşları da kapsamaktadır.

Tüm paydaşlar farklı roller üstlenmekte ve farklı rolleri bünyesinde barındırmaktadır. Örneğin bir kişi mevzubahis faaliyete göre yurttaş, tüketici, ebeveyn, öğrenci, işçi vs. olabilir. Kurumların çoğu dijital ortam kullanıcılarıdır. Temel faaliyetlerinin bir parçası olarak bazıları dijital ortamın işletilmesiyle, yönetimiyle ya da tasarımıyla ilgilenmektedir (örneğin yazılım ya da donanım üreticisi, telekomünikasyon işletmesi ya da İnternet servis sağlayıcısı). Belli bir büyüklüğün üzerindeki kurumlar genellikle kurumun faaliyetlerini desteklemek için gerekli olan dijital altyapıyı sunmaktan sorumlu bir Bilişim Teknolojisi (IT) departmanına sahiptir. Bazı bireyler de uygulama ya da yazılım geliştiricileri gibi, belli bir kurumun parçası olmadan dijital ortamın işletmesine dahil olabilmektedir. Hükümetler de farklı rolleri bünyesinde barındırabilir: onlar da dijital ortamın kullanıcıları olup ortama oldukça bağlı durumdadır (örneğin e-devlet uygulamalarının yanında memurların maaşını ödemek gibi çoğu devlet işlevlerini yerine getirmek için); bunun yanında dijital ortamla da alakalı olacak şekilde ekonomik ve sosyal refahı teşvik edecek kamu politikalarını hayata geçirirler.

Dijital güvenlik riski

Tavsiye Metninden alıntı (VII.1):
"Risk, belirsizliklerin hedefler üzerindeki etkileri olarak tanımlanmaktadır. "Dijital Güvenlik Riski", herhangi bir faaliyetteki dijital ortamın kullanımı, geliştirilmesi ve yönetimi ile ilgili risk kategorisini tanımlamak için kullanılmaktadır. Bu risk dijital ortamdaki tehditlerin ve açıkların bileşimi neticesinde ortaya çıkabilir. Bu risk, ilgili faaliyet ya da ortamın gizliliğini, bütünlüğünü ve bulunabilirliğini bozarak ekonomik ve sosyal hedeflerin gerçekleştirilmesini sekteye uğratabilir. Dijital güvenlik riski doğası gereği dinamik bir yapıdadır. Dijital ve fiziksel ortamlar, faaliyetle ilgili bireyler ve faaliyeti destekleyen organizasyon süreçleri ile ilgili bileşenleri barındırır."

Paydaşların hedeflerini gerçekleştirmek üzere yürüttükleri faaliyetler, başarı olasılıklarına göre sonuçları olabilen faktörlere bağlıdır. Belirsizlik insan yaşamının bir parçasıdır: bu faktörleri ve onların hedeflerimizi nasıl etkileyebileceğini bilmemiz ve anlamamız sınırlıdır. "Risk", belirsizliklerin paydaşlar tarafından gözetilen hedeflerin üzerindeki etkileri ya da sonuçlarıdır; yani gerçeklerin beklentiler üzerinde empoze ettikleri belirsizliklerdir. Bu risk yaklaşımı ISO/IEC 31000:2009, ISO/IEC 27000 serisi ve ISO Rehberi 73'e dayanmaktadır (bkz. Kutu 3). Risk genellikle olasılık ve etki gibi terimlerle ifade edilmektedir ve risk düzeyleri genellikle bu iki boyutun farklı kombinasyonlarını dikkate alabilmek adına X-Y ekseninde gösterilmektedir.

Tavsiye Metninde tanımlandığı üzere (bkz. Kutu 3) dijital güvenlik riski, paydaşların karşı karşıya oldukları birçok risk kategorisinden biridir. Dijital güvenlik riski:

- *Tek başına olmamak kaydıyla "dijital belirsizliğe" bağlıdır.* Bilgi ve İletişim Teknolojisine bağımlılığın olduğu her durumda, buna bağlı olarak aynı zamanda dijital ortamın kullanımı ile ilgili belli bir belirsizlik seviyesi mevcuttur ("dijital belirsizlik"). Ancak, dijital güvenlik riski sadece "sıfırlar ve birler" ile ilişkili değildir: dijital ortama bağlılık yazılım, donanım ve doğrudan ya da dolaylı insan müdahalesi ya da etkileşimi gerektirmekte olup, bunların tümü tehditlere, açıklara ve vakalara tabidir. Örneğin, bir hizmetin sürekliliği ya da bir üretim bandı, veri merkezine sağlanan enerjinin doğal bir afet nedeniyle ya da enerji kablolarının tahrip edilmesiyle kesintiye uğrayabilir. Ticari sırlar, manipüle etmek ya da kandırmak suretiyle insanları bilgi sistemlerine yasal olmayan şekilde girebilmek için bazı eylemleri yapmalarına neden olabilmelerine yol açan sosyal mühendislik teknikleri kullanarak suçlular tarafından çalınabilir. Yani tehditlerin, açıkların ve vakaların dijital yönlerinin yanında fiziksel ya da insan faktörü boyutu da olabilmektedir.

Kutu 3. Tanımlar, terminoloji ve standartlar üzerine

Tavsiye Metninde kullanılan terimler ve tanımlar kuralcı ya da katı bir bakışla ya da belli bir risk terminolojisini destekleyici ya da diğer tanım ve terimlerden üstün olarak algılanmamalıdır. Bunlar yüksek düzey politik rehberlik için destek sunmak ve OECD içinde ve ötesinde farklı ekonomik, sosyal ve politik durumların yanında farklı ülkeler, kültürler, hukuki rejimlerden gelen liderler ve karar alıcıları kitlesine hitap etmek üzere seçilmişlerdir.

Mümkün olduğu sürece Tanım Metnindeki risk terminolojisi ISO/IEC uluslararası risk yönetimi standartları ve rehber esaslarına ve özellikle de ISO/IEC 31000:2009 ve ISO Rehberi 73 (ISO/IEC 27000 serisinde de yansıtıldığı üzere) belgelerine dayanmaktadır. Bununla beraber bazen farklı terminoloji de kullanan daha birçok başka risk ile ilgili standartların olduğunu kabul etmektedir[25]. Çoğu durumda terimler ve tanımlar Tavsiye Metninin hedef kitlesi, amaçları ve kapsamlarına göre düzenlenmiştir. Tavsiye Metninde de belirtildiği üzere İlkelerin halihazırdaki risk yönetimi süreçleri, en iyi uygulamaları, metodolojileri ve standartları ile uyumlu olması gözetilmiştir. Tavsiye Metninin liderler ve yüksek düzey karar alıcılar ile bu standartları uygulamadan sorumlu uzmanlar arasında sosyal ve ekonomik refahtan faydalanabilmek adına bir köprü kurabilmesi beklenmektedir.

Risk yönetimi sağlıktan finansa, mühendisliğe, sigortacılığa ve endüstriyel süreçlere kadar her birinin kendi risk kültürü, terminolojisi ve standartları olduğu birçok farklı sektöre uzanan karmaşık bir alandır. Tavsiye Metni kesin ve kapsayıcı bir risk ve risk yönetimi anlayışı sunma iddiasında değildir. Risk, tarih boyunca sürekli evrime uğramış olan eski bir kavram olup hala da değişime açıktır. Risk ya da risk terminolojisi için herkes tarafından kabul görmüş tek bir tanım yoktur: bir araştırmacı 27'den fazla risk tanımını analiz edip dokuz kategoriye ayırmış, aynı zamanda büyük olasılıkla daha da fazla tanımın mevcut olabileceğini belirmiştir (Aven, 2012)

- *Ekonomik ve sosyaldir.* Dijital belirsizliğin etkileri ya da sonuçları ekonomik ve sosyal olmaktadır ve menkul ya da gayrimenkul varlıkları etkileyebilmektedir. Bu yüzden risk sosyal ve ekonomik terimler üzerinden formüle edilmelidir: mali kayıp, rekabet kaybı, fırsat kaybı, itibar, imaj ya da güven zedelenmesi vs. Bağlamına göre, Tavsiye Metninin kapsamının dışında kalan başka etkiler de (yani risk kategorileri de) ortaya çıkabilmektedir ve bunların da bir şekilde ele alınması gerekmektedir. Örneğin kurumlar sadece teknik (yani BİT) boyuttaki sonuçları ele alabilir ve hükümetler de ulusal ve uluslararası güvenlik ile ilgili sonuçlarla ilgilenebilir.

- *Sürekliliği, bütünlüğü ve gizliliği* (yani "güvenliği") *etkiler*. Bu tip etkilere sahip olaylar, faaliyetlerin ya da bu faaliyetlerin yapıldığı ya da dolaylı ya da doğrudan bağımlı oldukları dijital ortamın sürekliliğinin, bütünlüğünün ve gizliliğinin bozulmasıdır. "AIC üçlemesi" olarak adlandırılan bu durum, dijital güvenlik risk yönetimi kapsamını özel bir alan ve uzmanlık kategorisi olarak şekillendiren klasik güvenlik özellikleri ya da niteliklerini ortaya koymaktadır. Yani, örneğin, dijital güvenlik riski, dijital ortamdaki fikri mülkiyet hakları ihlaline ya da uygunsuz bilgilerin (içeriklerin) yayılmasına ilişkin belirsizlikleri kapsamamaktadır[23].

- *Olumsuz etkisi vardır*. Günlük dilde "risk", genellikle belirsizliğin zarar verici etkilerini ifade etmektedir; buna paralel olarak Tavsiye Metni de ekonomik ve sosyal hedeflerin gerçekleştirmesine ket vurabilecek belirsizliklere odaklanmaktadır. Dijital güvenlik risk yönetimine ekonomik ve sosyal hedefleri en iyi şekilde yerine getirebilmek üzere değerleri koruma aracı olarak yaklaşmaktadır. Ancak, belirsizlikler aynı zamanda faaliyete yararı dokunabilen olumlu sonuçlar da doğurabilmektedir. Belirsizliklerin olumlu sonuçları genellikle riskten ziyade "fırsat" olarak adlandırılmaktadır. Dijital güvenlik risk yönetiminin, inovasyonu teşvik etmek için sistematik olarak belirsizlikleri tespit etmek ve bunlardan faydalanmak yoluyla *değer üretmede* de kullanılabildiğinden, risk ile fırsat arasındaki ilişki oldukça önemlidir. Bu durum aşağıda (İnovasyon İlkesi) daha ayrıntılı olarak ele alınmıştır.

Risk faktörleri: tehditler, açıklar ve vakalar

Risk, tehditlerle açıkların birleşmesi neticesinde, ekonomik sonuçlar meydana getiren olaylarda ortaya çıkabilmektedir. Faaliyetlerin beklenen seyrini değiştiren ve hedeflere etki eden olaylara genellikle *vaka* denmektedir. Faaliyete etki eden sonuçların ortaya çıkması için hem tehditlerin hem de açıkların bulunması gereklidir. Tehdit olmadan açıklar ya da açık olmadan tehditler tek başlarına riski artırmamaktadır. Günlük dilde "risk" kelimesi daha serbest anlamda kullanılmaktadır. Örneğin, risk aynı zamanda tehdit, açık, vaka, olasılık, şans vs. gibi anlamlara gelebilmektedir[24]. Ancak risk yönetimi, nedenler ve sonuçları kesin bir şekilde ayırt etmeyi gerektirmektedir; bu yolla nedenlere (tehditler, açıklar ve vakalar) müdahale ederek sonuçları (risk) kontrol altına alabilmektedir. Bu farkı vurgulamak için tehditler, açıklar ve vakalar bu metinde "risk faktörleri", yani riski oluşturan ya da katkı sağlayan nedenler olarak adlandırılmaktadır.

Tehditler genellikle faaliyetin dışından kaynaklanmakla beraber açıklar ve zafiyetler genellikle faaliyete içkindir. Bunun sonucu olarak paydaşların genellikle tehditleri etkileme

kabiliyeti sınırlıdır ve genellikle açıklar üzerinde harekete geçmektedirler. Bazı durumlarda hem tehdit hem de açık faaliyetin içinden gelebilmektedir; tıpkı hoşnutsuz bir çalışanın kendi imtiyazlarını kullanarak uygunsuz işlemlerde bulunması ve işveren için zarar verici sonuçlara neden olması gibi.

Tehditler, açıklar ve vakalar için birçok kategori ve sınıflandırma mevcuttur. Örneğin bir tehdit bilerek (yani saldırı, suçluların bir şey çalmaya çalışması gibi) ya da bilmeyerek (yani bir kaza sonucu, yol inşası esnasında fiber optik kabloların kesilmesi gibi) oluşturulabilir. Bir vaka, bilmeden yapılan hatalar ya da sosyal mühendislik teknikleri ile (örneğin phishing) kişilerin yönlendirilmesi gibi insanların eylemlerinden ya da fırtına, sel, deprem gibi doğal afetlerden kaynaklı olarak oluşabilmektedir. Bilerek meydana getirilen tehditlerin karmaşıklık seviyesi, uluslararası tehditlerin kaynağının genç ergenlerden devlet destekli gruplara kadar değişen kaynaklarının da gösterdiği üzere çok basitten oldukça karmaşığa kadar gidebilir. Son olarak vakaların süresi de yılın en yüksek satış döneminde müşterilerle olan iletişim kanallarını bozmak yoluyla gerçekleştirilen ani hizmet engelleme saldırısı gibi oldukça kısa; ya da bir şirketin ticari sırlarını çalarak o şirketi piyasadan silmek için bilgi sistemlerine gizli sızma yapmak gibi oldukça uzun (yıllara varan) süreli olabilmektedir.

Dijital güvenlik riskinin dinamik yapısı, tüm bileşenlerinin sürekli değişen özelliklerinden kaynaklanmaktadır: ekonomik ve sosyal faaliyetler, risk faktörleri ve dijital ortam.

Dijital güvenlik risk yönetimi

Tavsiye Metninden alıntı (VII. 2):
“‘Dijital güvenlik risk yönetimi”, belli bir kurum dahilinde ve/veya kurumlar arasında dijital güvenlik riskine karşı alınan, aynı zamanda olanakları maksimize eden bir dizi eşgüdümlü eylemdir. Hem karar alma sürecinin, hem de ekonomik ve sosyal faaliyetlerdeki genel risk yönetimi çerçevesinin bir parçasıdır. Bütünsel, sistematik ve esnek bir dizi döngüsel ve aynı zamanda olabildiğince şeffaf ve açık olan süreçlere dayanmaktadır. Bu süreçler dizisi, dijital güvenlik risk yönetimi önlemlerinin (“güvenlik önlemleri”) ilgili risk ve ekonomik ve sosyal hedeflere göre uygun ve orantılı olmasını sağlamaya yardımcı olur.”

Dijital risk tamamen ortadan kaldırılamaz (Kutu 2’de ifade edildiği üzere), ancak ekonomik ve sosyal faaliyetleri korumak ve desteklemek adına yönetilebilir. Yani, dijital güvenlik risk yönetimi ekonomik ve sosyal hedeflerin gerçekleşmesine yardımcı olmayı amaçlamaktadır. Bununla beraber dijital risk yönetimi aşağıdaki özelliklere sahiptir:

- *Ekonomik ve sosyal karar alma süreçlerinde stratejik öneme sahiptir.* Risk yönetimi karar vericilerin faaliyetleri tasarlarken ve gerçekleştirirken hedeflere ulaşılmasını etkileyebilen faktörleri dikkate aldığı süreçtir. Ekonomik ve sosyal faaliyetlerin dijital ortama doğrudan ya da dolaylı bağlı olduğu ölçüde dijital risk yönetimi karar alma sürecinin bir parçası olmalı ve fırsatları maksimize etmek üzere geliştirilen stratejilerle birlikte ele alınmalıdır (bkz. İnovasyon İlkesi). Liderlerin dijital güvenlik risk yönetimini tamamen teknik bir uğraşı olmaktan ziyade sosyal ve ekonomik boyutlarının da olduğunu da görmeleri gerekmektedir. Ancak, bazı BİT güvenlik açıkları, bir takım olası BİT güvenlik vakalarının özellikleri (örneğin yayılma ve yükselme potansiyelleri) gibi ana risk faktörlerini ve bunun yanında riske müdahale için gerekli olabilecek BİT tedbirleri gibi çeşitli önlemleri tespit edebilmek için dijital ortamı işleten ve idame ettiren uzmanlar gibi diğer paydaşlarla işbirliği içinde olmaları

gerekmektedir. BİT uzmanları teknik düzeyde riskleri tespit edip müdahale edebilirler, ancak vakaların ve onlar için alınan teknik önlemlerin kuruma olan ekonomik etkilerini analiz edemezler. Buna benzer bir şekilde sadece liderler ve karar alıcılar dijital güvenlik riskini kurumun bütünsel stratejik hedefleri ve planları doğrultusunda ele alabilirler.

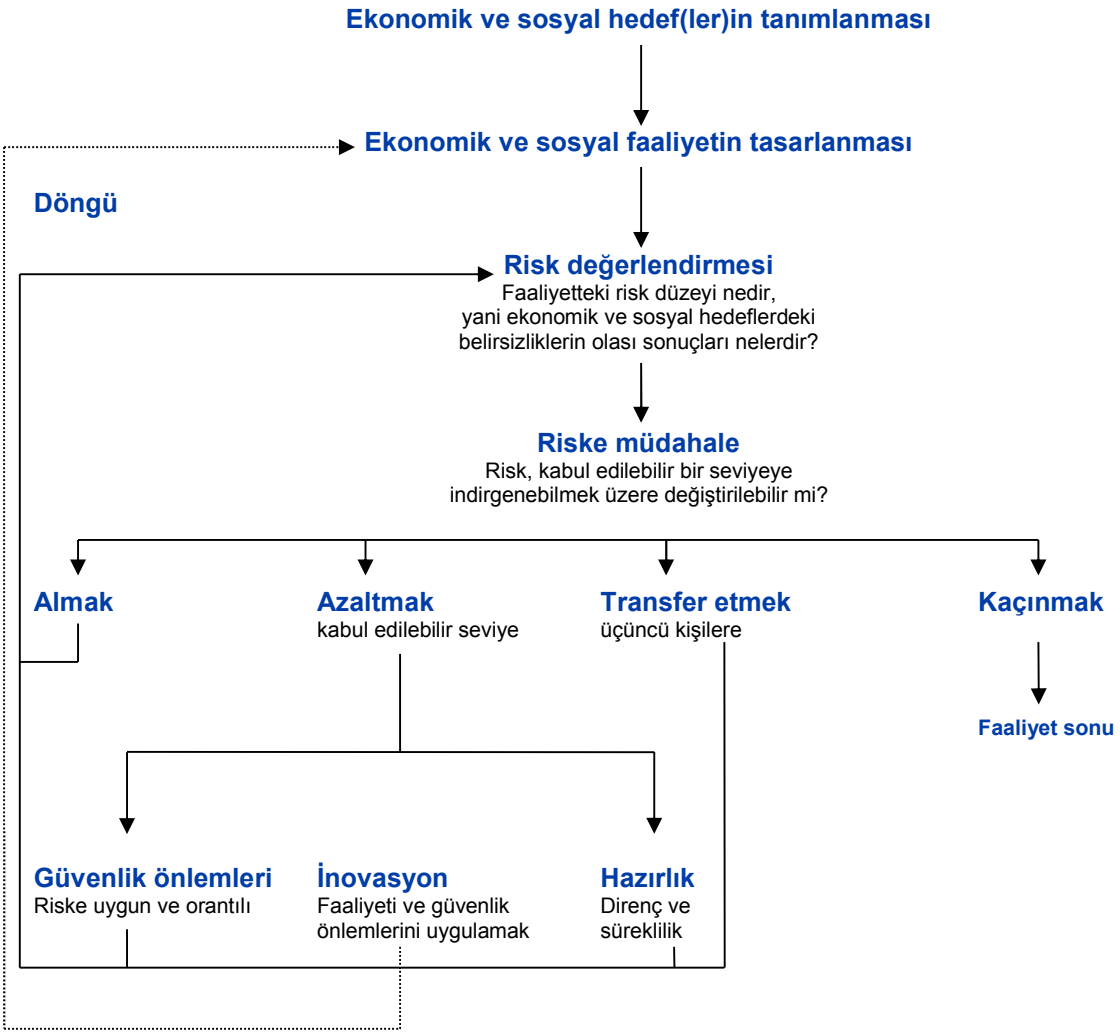
- *"Güvenlik önlemlerinin" ilgili ekonomik ve sosyal faaliyet tamamen desteklemesini sağlar ve faaliyetleri engellemez.* Bir faaliyeti tüm tehditlerden, açıklardan ve vakalardan tamamen korumak imkansızdır. Bu nedenle, dijital güvenlik risk yönetimi önlemlerinin ("güvenlik önlemleri") seçimi ve uygulanması ile ilgili bir takım seçimlerin yapılması gerekmektedir. Ayrıca, güvenlik önlemleri korumayı hedefledikleri faaliyet ile ilgili olarak tamamen tarafsız olamamaktadır. Güvenlik önlemleri ilgili faaliyet için farklı türde engeller ve sınırlamalar ortaya çıkarabilmektedir. Örneğin, finansal maliyeti, sistemin karmaşıklığını ve pazarlama süresini artırabilir, aynı zamanda performansı, kullanılabilirliği, gelişme kapasitesini, inovasyonu ve kullanıcı kolaylığını azaltabilirler. Önlemler ayrıca gizlilik tehditleri (bkz. Kutu 4) ve diğer farklı olumsuz sosyal sonuçlara neden olabilmektedir. Bu sınırlamalar ve olumsuz etkiler müdahale edilebilir ve azaltılabilir, ancak bu beraberinde bir maliyet getirmektedir. Dijital güvenlik risk yönetiminin temeli ilgili faaliyetin ekonomik ve sosyal gerçekliğindeki güvenlikle ilgili kararlara dayanmaktadır. Kararların izole bir şekilde, ayrı bir teknik ya da güvenlik bakış açısıyla alınmasını engellemektedir. "Güvenlik önlemlerinin" ilgili risk ve faaliyete uygun ve orantılı olarak seçilmesi amacını gütmektedir. Bu şekilde, güvenlik önlemlerinin ekonomik ve sosyal faaliyetleri desteklemesini sağlamakta ve örneğin dijital ortamın uygunsuz bir şekilde kapatılması ya da işlevselliğinin düşürülmesi gibi eylemlerle BİTlerin inovasyona ve üretkenliği arttırmaya olan etkilerinden faydalanabilme olasılığını sınırlama yoluyla faaliyetlerin daha fazla engellenmesini önlemektedir.

- *İzole ve ayrı bir alan olmaktan ziyade, genel risk yönetimi çerçevesinin bir parçasıdır.* Dijital güvenlik riski ekonomik ve sosyal faaliyetleri etkileyen birçok risk kaynağından sadece bir tanesidir. Dijital güvenlik risk yönetimini daha geniş, kurumsal bazda risk yönetimi çerçevesine dahil etmek, risk ortamının liderler ve karar alıcılar için daha bütüncül bir resmini ortaya koyabilmesini ve bu yolla daha stratejik ve etkili liderlik ve karar alma süreci oluşturulmasını sağlamaktadır. Dijital güvenlik riski için halihazırdaki risk yönetimi çerçevesinin dışında özel bir risk yönetimi çerçevesi oluşturmak üretkenliğe zarar verici niteliktedir.

Tipik bir risk yönetimi döngüsü, faaliyetlerin yürütülmesi ve faaliyetlerin süresi boyunca devam etmesi açısından karar alma sürecinin bir parçası olmalıdır. Şekil 1, Tavsiye Metnindeki İşletim İlkelerini yansıtacak şekilde risk yönetiminin genel bir betimlemesini sunmaktadır. Süreç hedeflerin ve faaliyetlerin tasarımının tanımı ile başlamaktadır. Daha sonra risk değerlendirilmekte ve bu değerlendirmeye göre ve hedefleri destekleyecek ve koruyacak şekilde riske müdahale edilmektedir. Riske müdahale, faaliyetin başarıya ulaşması olasılığını arttırmak için riskin değiştirilip değiştirilemeyeceği ve değiştirilebilecekse bunun nasıl yapılacağını, yani riskin hangi kısmının alınması, azaltılması, transfer edilmesi ya da kaçınılması (İlke 1) gerektiğine karar verileceğini belirlemektedir. Riski azaltmak için güvenlik önlemleri seçilebilir ve uygulamaya konulabilir (İlke 2), inovasyon hem güvenlik önlemleri hem de ilgili faaliyet açısından dikkate alınabilir (İlke 3) ve hazırlık önlemleri

tanımlanabilir ve bir vaka meydana geldiğinde uygulamaya konulabilir (İlke 4). Uygulama İlkeleri ile ilgili bölümde bununla ilgili daha fazla ayrıntı sunulmaktadır.

Şekil 1: Dijital güvenlik risk yönetimi döngüsüne genel bakış



Not: Risk yönetim döngüsünü ifade etme biçimlerinden bir tanesi gösteren bu şekil, Tavsiye Metnindeki Bölüm 1'de sunulan Uygulama İlkeleri kısmına odaklanmaktadır. Genel İlkeler, döngüyü destekleyen kaideler olarak ele alınmalıdır.

Kaynak: OECD.

Göreli olarak daha büyük kurumlarda, dijital güvenlik risk yönetiminin karmaşıklığı nedeniyle kurum içinde bütünsellik ve tutarlılık sağlayabilmek adına resmi bir çerçevenin benimsenmesi gerekmektedir. Genelde şirket ya da kurumsal politika ya da yönetim belgesi formatında yansıtılan bu çerçeve, kurumun kültürüne ve yönetim stiline bağlı olarak birçok şekli alabilmektedir. Bu çerçeve, kurumun halihazırdaki toplam risk yönetimi çerçevesiyle tutarlı ve onun bir parçası olup aynı zamanda Tavsiye Metnindeki İlkeleri de yansıtmaktadır.

Bu tür bir çerçeve genellikle tüm ilgili paydaşların katılımı ile oluşturulur ve maksimum tutarlılık ve görünürlük adına en üst düzeyde benimsenir. Bu durum, bu metinde ele alınmayan ve daha detaylı bir incelenmenin yararlı olabileceği bir dizi karmaşık yönetim meselelerinin ortaya çıkmasına neden olabilmektedir. Genelde, çerçeve onu uygulamakla yükümlü olan aktörlerin sorumluluklarını ve hesap verebilirliklerini açık bir şekilde resmeder. Çerçevenin ele alabileceği önemli bir nokta da kurum içindeki "iş" ve BİT liderliklerinin dijital risk yönetimi için el ele verip işbirliği içinde olmasını sağlayacak yöntemlerdir.

Çerçeve, kurumun yaşam döngüsü boyunca dijital ortama bağımlı olan tüm ekonomik ve sosyal faaliyetlerinin tüm boyutlarıyla içermektedir. Riske devamlı sistematik bir şekilde yaklaşılmasını sağlamak adına kurumsal süreçleri açıkça belirler. Ortaya çıkabilecek dijital güvenlik risklerine hızlı ve ileriye dönük bir müdahalede bulunabilmeyi sağlamak için esnek niteliktedir. Aşağıda da açıklandığı üzere (Uygulama İlkeleri), çerçeve bütünsel, sistematik ve esnek bir takım süreçlerin riskin içsel olarak dinamik olan yapısı ile uyum sağlayabilmek adına uygulanmasını sağlamaktadır. İyi uygulamaları ve standartları dikkate alırken bir yandan da bu uygulamaların ve standartların kapsamının dışında olabilecek bağlama özel unsurları de ele almaktadır. Bir şeffaflık düzeyi, kurumun dijital güvenlik riskine hitap etmeye yönelik taahhüdünün kanıtı olarak kurum içinde ve dışında itibar ve güven artışını sağlamaktadır. Bu şekildeki bir çerçeve, örneğin "yaptığın şeyi yaz, yazdığın şeyi yap" gibi basit kurallara uyulmasını teşvik ederek kolaylıkla ve bağımsız olarak doğrulanabilir olmalıdır. Çerçevenin sürekli bir döngü içinde gözden geçirilmesi ve iyileştirilmesi risk yönetiminin etkili olabilmesi ve güveni arttırmak açısından çok temel bir öneme sahiptir. Bu genelde önlemleri yerinde test etmek, denetlemek ve optimize etmek adına kullanılan süreçleri kapsamaktadır.

Dijital güvenlik risk yönetiminin döngüsel yapısı ile ilgili ve benzeri diğer ayrıntılar Uygulama İlkeleri adlı bölümde sunulmaktadır.

Kutu 4. Dijital güvenlik risk yönetimi ve gizlilik

Dijital güvenlik risk yönetimi ve gizliliğin korunması arasındaki ilişkinin en az üç farklı boyutu bulunmaktadır.

İlk olarak dijital güvenlik risk yönetimi, veri denetleyicilerinin (kişisel verilerin içeriği ve kullanımını belirleyen taraflar) "kişisel veriler uygun güvenlik önlemleriyle veri kaybı ya da yetkisiz erişim, yok etme, kullanım, değiştirme ya da ifşa gibi risklere karşı korunmalıdır" şeklinde ifade edilen OECD Gizlilik Ana Esaslarındaki Güvenlik Önlemleri İlkesini uygulayabilmeleri adına sağlam bir temel sunmaktadır.

Dijital güvenlik risk yönetimi özellikle "uygun" güvenlik önlemlerini tanımlarken etkili bir yaklaşım olan güvenlik önlemlerinin risk ile uyumlu ve orantılı olmasını sağlamaktadır. Ancak veri denetleyicilerine göre kişisel verilerle ilgili kabul edilebilir risk seviyesi verinin ilgilendirdiği veri öznesinin kabul ettiği seviyeden daha yüksek olabilmektedir. Gizliliğin korunması ile ilgili önemli bir nokta veri öznesin çıkarları ile veri denetleyicisinin çıkarları arasındaki olası uyumsuzluklardır. Daha genel olarak, risk değerlendirmesini yürüten tarafın (veri denetleyicisi) risk ile karşı karşıya olan (veri öznesi) taraf olmaması güvenlik ve gizlilik risk değerlendirmesi arasındaki en önemli farktır.

Buna ek olarak, dijital güvenlik risk yönetimi, örneğin ağların izlenmesi, ya da risk ile bilgilerin üçüncü taraflarla paylaşılması gibi gizlilik riskini arttıran güvenlik önlemleri getirerek gizliliğe zarar verebilmektedir. Gizliliğin korunması Tavsiye Metnindeki insan hakları ve temel değerler ile ilgili olan ve başkaların hukuki çıkarlarına saygılı olma ve gözetme çağrısında bulunan Bölüm 1'de üçüncü İlkeye dahil edilmiştir.

Son olarak risk yönetiminin Gizlilik Ana Esaslarında belirtilen İlkeleri daha iyi bir şekilde uygulayabilmek için kullanışlı bir metodoloji sunduğu giderek daha fazla kabul görmektedir. Yine de pratik uygulamaların ve sonuçlarının tam olarak anlaşılabilmesi için daha fazla çalışmanın yapılması gerekmektedir.

İlkelerin Uygulanabilirliği

İlkeler, paydaşlarca, kendi rollerine, yetkinliklerine ve bağlama göre uygulanmalıdır (IV). Bu genelde tüm İlkeler için geçerli olsa da özellikle Sorumluluk İlkesi ile ilgili olarak önem arz etmekte ve Uygulama İlkelerinin uygulanabilirliği üzerinde sonuçlar doğurmaktadır.

Roller: kullanıcıların dijital ortamdan sorumlu paydaşlardan ayırt edilmesi

Tanımda da belirtildiği üzere, paydaşlar farklı rollere sahip olabilmekte ve birden fazla rol üstlenebilmektedir. Önemli bir ayrım, genel olarak paydaşlar ile dijital ürün ve hizmetleri geliştiren ve yayan kişiler arasında yapılmalıdır. Tüm paydaşlar, dijital ortamın kullanıcısı konumundadır ve bununla beraber kendi faaliyetlerine ilişkin dijital güvenlik risk yönetiminde bulunmaları gerekmektedir. Ancak, bunlar arasında dijital ortamın geliştirilmesi ve idare edilmesinden sorumlu olanlar (örneğin BİT uzmanları), aynı zamanda mümkün olduğunca[27] kullanıcılarının dijital güvenlik riskini yönetebilmelerini sağlamak adına ürün ve hizmetlerinde uygun güvenlik önlemlerini uygulamaları gerekmektedir. Bu yüzden dijital güvenlik risk yönetiminde ikili bir kültür oluşturmalıdırlar: ilki dijital ortama bağlı olan kendi faaliyetleri ile ilgili riske hitap etmeli, ve ikincisi de tüketicilerin ve kullanıcıların dijital ortamı kullanmalarında ortaya çıkacak riskin yönetimine yardımcı olmak için uygun araçlar sağlayabilmek adına ürün ve hizmetlerini optimize etmeyi hedeflemelidir. Örneğin, tüketicilerin halihazırda ürün ve hizmetlerin içine dahil edilmiş anlayabilecekleri ve kullanabilecekleri güvenlik özelliklerine sahip, kullanıcı dostu ve varsayılan ayarlardan faydalanan bir şekilde ürün ve hizmetleri tasarlayabilirler.

Bu iki olgu birbiriyle alakalıdır: BİT ürün ve hizmetlerinin geliştirilmesiyle ilgili güvenlik riskinin
düzgün yönetilememesi bu ürünlere ve hizmetlere yerleştirilmiş olan güvenlik önlemlerinin etkinliğini etkileyebilmekte ve bu da kullanıcıların riskini yükseltebilmektedir. Örneğin, Hollanda Belgelendirme Kuruluşu olan DigiNotar'ın bilişim sistemlerine 2011'de bir sızma olmuş, bu da 300000 Gmail hesabına karşı saldırıya olanak vermiş, bunun sonucu DigiNotar'ın müşterilerinin güvenlik riski artmış ve nihai olarak bu şirkete (şirket en sonunda iflas etmiştir) dolaylı olarak bağımlı olan Hollanda e-devlet altyapısına olan güveni sarsmıştır. Başka bir örnekte de, 2011 yılında bir güvenlik şirketi olan RSA'da vuku bulan, 40 milyon şifrematiğe sızıldığı ve çalınan bilginin kullanılması suretiyle savunma sektöründeki müşterilere saldırılar düzenlenmesine yol açan sızmadır[28]. BİT sektöründeki paydaşların, BİT güvenlik sektöründekiler en başta olmak üzere dijital güvenlik risk yönetiminde örnek teşkil edecek nitelikte olması gerekmektedir.

Yetkinlik: KOBİleri ve bireyleri diğer paydaşlardan ayırt etmek

Paydaşların yetkinlikleri, diğerlerinin de yanında özellikle şu faktörlere dayanmaktadır: i) Genel dijital güvenlik risk anlayışları; ii) Bu uğraşı için sarf edebilecekleri ehemmiyet ve kaynak miktarı; iii) Bazen "otorite" olarak da adlandırılan hukuki yetkinlikleri; ve iv) dijital ortamı denetleyebilme düzeyleri ve bunu yapabilme rahatlıkları. Bu dört faktörle ilgili olarak, hükümetler ve büyük ölçekli kurumlar, yetkinlikleri daha sınırlı olarak kabul edilen KOBİler

ve özellikle de bireylerden ayırt edilmeleri gerekmektedir. Özellikle KOBİlerin ve bireylerin sergileyebildikleri kontrol seviyesi, piyasada bulabildikleri dijital ürün ve hizmetlerdeki güvenlik önlemlerinin bulunabilirliği, satın alınabilirliği, kullanılabilirliği ve uygunluğu faktörlerine bağlıdır[29].

Bu sınırlamaları göz önüne alarak, Tavsiye Metni hükümetleri ve kamu ve özel sektör kurumlarını bireylerin ve KOBİlerin dijital risk yönetimini uygulayabilmeleri için güçlendirmek adına birlikte çalışması çağrısında bulunmaktadır (V). Dahası, kavramsal olarak tüm paydaşlar için önemli olsa da, Bölüm 1'deki Uygulama İlkeleri öncelikle belli bir büyüklüğün üzerindeki kurumların dijital güvenlik risk yönetimi çerçevelerini oluşturabilmeleri adına tasarlanmıştır. Tavsiye Metninin kabulünden sonra, bu İlkelerin bireyler ve KOBİler üzerindeki pratik ve kamu politikaları açısından etkilerini daha iyi anlamak ve mümkün olursa bu doğrultuda rehberlik sağlamak adına daha fazla çalışma yapılması beklenmektedir.

Bağlam: özel durumları ayırt etmek

İlkelerin yorumlanmasında bağlam önemli bir yer tutmaktadır. Hukuki ya da düzenleyici koşullar, örneğin dijital güvenlik risk yönetiminin nasıl uygulanacağını, kritik hizmetleri sağlayanların resmi bir risk değerlendirmesi yapmalarını ve uygun önlemlerin yerleştirilmesini sağlayarak etkileyebilmektedir. Buna ek olarak, Uygulama İlkeleri KOBİler ve bireyler için sınırlı yetkinliğe sahip olmalarından dolayı özel bir yorumlama gerektirirken, bazıları dijital güvenlik risk yönetiminin önemini arttıran bağlamlarda uygulanabilmektedir. Bunlara örnek olarak kritik sektörlerdeki KOBİler, ya da doktor ya da gazeteci gibi yüksek derecede hassasiyet gerektiren verilerle uğraşan bireyler gösterilebilir.

Kurumsal yapı dışında dijital ortam bileşenlerini geliştiren ve bakımını yapan bazı bireylerin paydaş olarak hareket edebildiklerini belirtmekte yarar vardır. Bu, örneğin milyonlarca kişi tarafından kullanılan temek güvenlik bileşenlerini (örneğin OpenSSL, ya da GNU Gizlilik Koruyucu [GPG][30]) geliştiren, bazen bu araçlar üzerinde gönüllü olarak ya da çok sınırlı bütçelerle ve destekle çalışan kişiler için geçerli bir durumdur. Bu durum aynı zamanda bir ankete göre uygulamalarından ayda 500 dolardan az kazanan uygulama geliştiricilerinin büyük bir çoğunluğu için de geçerlidir[31].

İlkeler

İlkelerin genel yapısı

Sekiz adet olan İlkeler "bir bütün olarak ele alınmalıdır"[32]: hepsi de vazgeçilmezdir ve her biri tek başına uygulanır ya da yorumlanırsa ya da aralarından biri göz ardı edilirse etkili olmaktan çıkmaktadır. Sıralanmaları ve numaralandırmaları önemden ziyade mantıksal anlatı dolayısıyladır. İlkeler iki parça halinde düzenlenmişlerdir:

- *Genel İlkeler (1'den 4'e) "tüm* paydaşlara, yani ekonomik ve sosyal faaliyetlerinin tamamı ya da bir kısmı için dolaylı ya da doğrudan olarak dijital ortama bağımlı olan hükümetlere, kamu ve özel sektör kurumlarına ve bireylere hitap etmektedir.

- *Uygulama İlkeleri (5'ten 8'e)*daha ziyade devlet yönetiminde ve kamu ve özel sektör kurumlarında en üst düzey yöneticiliklerinden dolayı kurumları uygun bir dijital güvenlik yönetimi idari çerçevesine doğru yönlendirme konumunda bulunan "liderler ve karar alıcılara" hitap etmektedir.

Genel İlkeler

Dört İlke, işlevsel bir dijital güvenlik risk yönetimi döngüsünün oluşturulabilmesi için gerekli temel zemini teşkil etmektedir.

1. Farkındalık, beceriler ve güçlendirme

Dijital güvenlik risk yönetimini yürütmek ilk olarak ilgili risklerin var olduğunun anlaşılması ve eğitim, deneyim ya da pratik yoluyla gerekli becerileri elde ederek sorumlu kararları verebilmeyi (güçlendirme) gerektirmektedir. Dijital güvenlik risk yönetimi yaklaşımının ilk aşaması bu nedenle farkındalık yaratmak ve paydaşlara risk yönetebilme gücü verebilmek için becerilerin elde edilmesinden ibarettir.

Tüm paydaşların dijital ortamda birbirine bağımlı olması dolayısıyla biri tarafından karşılaşılan riskin göz ardı edilmesi ya da riskin yönetilmesindeki beceri eksikliği, riski diğerleri için arttırabilmektedir[33]. Bu nedenle hedef kitleye bir güç kazandırmaya yönelik her türlü farkındalık oluşturma ve beceri geliştirme önlemi, bu farkındalık ve becerilerin etkili bir biçimde eyleme dönüştürülmesi halinde toplam risk düzeyinin düşürülmesine katkı sağlamada topluca bir olumlu etki göstermektedir.

Risk farkındalığı risk faktörleri, yani tehditleri açıklar ve vakalar farkındalığından farklıdır. Bir araba kazasının olası sonuçları – fiziksel yaralanma ve ölüm gibi – içgüdüsel olarak bilinebilirken, dijital ortamın karmaşıklığı vakalar ve sonuçları arasındaki bağı belirsizleştirmektedir. Örneğin çoğu insan elektronik cihazlarına virüs bulaşabileceğinin farkındadır ama kimlik hırsızlığının, finansal dolandırıcılığın ya da ticari sır hırsızlığının potansiyel sonuçlarını anlamayabilir. Virüs bulaşmış bir cihazın hizmet engelleme saldırısında

bulunmak üzere kullanılan bir botnetin parçası olması gibi başkalarını etkileyen sonuçlar ise daha az görünürdür. Bu yüzden, farkındalık oluşturma, sadece tehditler, açıklar ve vakalar gibi risk faktörleri üzerinden ziyade bunların olası ekonomik ve sosyal sonuçları (yani riskleri) üzerine odaklanmalıdır. Farkındalık oluşturma aynı zamanda paydaşların dijital ortamı kullanmaktan vazgeçmek yerine bu ortamın ekonomik ve sosyal faydalarından en iyi şekilde yararlanabilmek adına risk yönetiminde bulunmak için gerekli olan becerileri elde etmelerini de teşvik etmelidir.

Benzer bir şekilde, dijital güvenlik riski yönetim için uygun bir genel kültürün geliştirilmesi her katılımcının kendi rolü, yetkinliği ve bağlama göre risk değerlendirmesi ve yönetimi yapması için gereken farkındalık ve becerilerden farklıdır. Riskin, risk faktörlerinin, dijital ortamın kullanımının ve ilgili ekonomik ve sosyal faaliyetlerin dinamik yapısını dikkate almak oldukça önemlidir. Farkındalık oluşturmak ve beceri geliştirmek sonu olmayan eylemlerdir. Bunlar için risk yönetim döngüsünün bir parçası olarak devamlı süreçler gerekmektedir.

Bu İlke tüm paydaşlar için geçerlidir: hükümetler, kamu ve özel sektör kurumları ve hatta bireyler de dijital güvenlik risk yönetimi farkındalıklarını arttırabilir ve becerileri geliştirmeye katkı sağlayabilir. Kamu ve özel sektör kurumları kendi çevrelerini hedef alan ve bunların kendi risk yönetim çerçevelerini desteklemek adına girişimler oluşturabilmektedir. Bunlardan bazıları, özellikle de BİT sektörü ve STKlar halkı ve çocuklar, ergenler, öğrenciler, yaşlılar gibi özel kitleleri hedef alan farkındalık oluşturma girişimlerini destekleyerek önemli bir rol oynamaktadırlar. Bu girişimler her türlü medya organını, kursları, saha eğitimlerini vs. kullanmak suretiyle birçok farklı şekilde yapılabilmektedir. Tavsiye Metninde de öncelik olarak arz eden önemli bir hedef kitlesi de kendi kurumları içinde kültürel ve kurumsal değişiklikleri yönlendirmek için en uygun kişiler olan liderler ve karar alıcılarının kendisidir. Kamu politikaları açısından son on yıl içerisinde, genel farkındalığı arttırmak adına hem hükümetler hem de özel sektör tarafından hatırı sayılır miktarda girişimlerde bulunulmuştur[34]. Bu girişimler tüm kategorilerdeki ekonomik ve toplumsal aktörlere ulaşmaya devam etmeli ve uygun becerilerin elde edilmesini iyileştirmelidir.

Yeteri şekilde farkındalığı, becerisi ve gücü olan paydaşlar sorumluluk alabilmektedir (İlke 2).

2. Sorumluluk

Bir kimsenin eylemlerinin kendisinde ve başkalarında neden olduğu sonuçlarla yüzleşmesi toplumsal hayatın temel ilkelerinden biridir. Bu yüzden tüm paydaşların, yukarıda da açıklandığı gibi kendi rolleri, yetkinlikleri ve bağlama göre dijital güvenlik risk yönetiminde sorumluluk almaları gerekmektedir.

Bu İlke, sorumluluğun yasal sonucu olan ve hukuki rejimlere ve bağlama göre farklılık gösterebilen mükellefiyeti ele almamaktadır. Sorumluluk İlkesi daha ziyade Tavsiye Metninin girizgahında belirtildiği gibi "hükümetler, kamu ve özel sektör kurumları ve bireyler, dijital güvenlik risk yönetimi ve dijital ortamın korunması için rolleri, yetkinlikleri ve bağlama göre sorumluluğu paylaşmaktadırlar" ifadesini yansıtmaktadır. Dijital güvenlik risk yönetiminin tüm yönleri için tamamen başkalarına bağımlı olmak artık imkansız hale gelmiştir. Sorumluluk paylaşılmaktadır: herkesin bir düzeye kadar sorumluluğu bulunmaktadır. Tüm paydaşlar rollerini, yetkinliklerini ve bağlamı gözden geçirmeli ve nasıl bir sorumluluk üstlenmeleri gerektiğini belirlemelidirler.

Bu sorumluluk dijital ortamın diğer ortamlardan farklı olmadığını vurgulamaktadır: ekonomik ve sosyal hedefleri gerçekleştirebilmek için belli bir seviyedeki dijital güvenlik riskinin kabul edilmesi gerekmektedir.

Bir benzetme yapmak gerekirse, tüm paydaşlar karşılıklı olarak rollerine, yetkinliklerine ve bağlama göre yol güvenliğinden de sorumludur. Sürücülerin nasıl araba kullanılacağını öğrenmeleri ve temel güvenlik ilkelerine uymaları gerekmektedir: alkol almamak, hız sınırlarına uymak, emniyet kemerini takmak, diğer sürücüleri dikkate almak gibi. Araba üreticileri arabaları tasarım ya da mekanik hatalardan dolayı oluşabilecek kaza olasılığını olabildiğince azaltmak için tasarlamalı (yani yetersiz frenler gibi zaaflardan kaçınarak) ve koruma mekanizmaları (hava yastıkları, dikiz aynası vs. gibi güvenlik önlemleri eklemek gibi) yerleştirmelidirler. Yolları inşa edenlerin yolları tasarlarken olası kazaları dikkate alarak gerekmektedir: bariyerler, göbekli kavşak, trafik ışıkları, yol işaretleri gibi. Hükümetlerin araba kullanma, araba üretimi ve trafikler ilgili kurallar koyması ve uygulaması gerekmektedir. Aynı zamanda acil durum hizmetleri (yani hazırlık önlemleri) de sunmalıdırlar. Bu sorumlulukların herhangi bir noktasında oluşacak hatalar her bir taraf ve herkes için risk seviyesini arttırmaktadır.

Sosyal ve ekonomik hedeflerini gerçekleştirmek adına dijital ortamı kullanmaya karar veren paydaşlar (sürücüler) belli bir seviyedeki dijital güvenlik riskini, yani olası olumsuz sonuçları kabul etmektedir. Bu riski yönetmeleri, yani aşağıda sunulan dört Uygulama İlkesine göre riski kabul edilebilir bir seviyeye indirmeleri gerekmektedir. Aynı zamanda eylemleri ya da eylemsizlikleri hakkında açıklama sunabilmeleri de gerekmektedir (hesap verebilirlik).

Ancak sorumluluk ve hesap vermede tüm katılımcılar eşit konumda değillerdir. Riski örneğin bilgi, birikim, beceri, kaynak, araç, kontrol ve ilgili teknoloji bağlamında yönetebilmeleri gerekmektedir. Katılımcılar arasında riski tespit etme, değerlendirme ve yönetme becerileri oldukça farklılık gösterebilmektedir ve bazı tür katılımcıların (örneğin bireyler ve küçük işletmeler) örneğin önemli ölçüde daha fazla kaynağa erişimi olan katılımcılarla kıyaslandığında aynı seviyede risk tespit etmeleri, değerlendirmeleri ve yönetmeleri beklenmemelidir. Yukarıda da vurgulandığı gibi bu İlkenin bireyler ve KOBİler tarafından benimsemesini sağlayacak girişimler ve olası yollar hakkında daha fazla çalışma yapılması yararlı olacaktır.

Yazılım, donanım (yukarıdaki benzetmeye göre araba üreticileri) ve ağ altyapıları (yukarıdaki benzetmeye göre yol inşa edenler) gibi dijital ortam bileşenlerini geliştiren, işleten ya da yöneten paydaşlar kullanıcılarının sorumlu risk yönetimi kararları alabilmeleri için gerekli koşulları sağlamaları gerekmektedir. Bu da örneğin riskin dinamik yapısını da hesaba katarak normları ve iyi uygulamaları benimsemek, teknik bileşenlerin içinde uygun güvenlik önlemlerini yerleştirmek ve kullanıcılarını güçlendirmek üzere gerekli bilgi ve desteği sağlamak gibi eylemleri içermektedir.

Hükümetler de kendi adlarına ulusal stratejiler geliştirmeli ve tüm paydaşlar arasında dijital güvenlik risk yönetimin teşvik etmek adına kamu politikaları girişimlerini ve önlemlerini benimsemelidirler. Çoğu OECD hükümeti halihazırda yönetmelikler, yasalar (örneğin siber suçlar ve gizlilik için), müdahale kapasitesi (Bilgisayar Güvenliği Vakası Müdahale Ekibi, BGVMEler yoluyla), eğitim, kamu-özel kurum ortaklığı gibi alanlarla birçok temel işlevi yerine getirmektedir. Birkaç yıl önce politikalarını daha stratejik terimlerle formüle etmeye başlamışlar[35] ve örneğin bu iş için ayrılmış ajanslar ya da diğer yollar vasıtasıyla yeni ya da

iyileştirilmiş işbirliği mekanizmaları oluşturarak yaklaşımlarının tutarlılığını arttırmışlardır. Bölüm 2'de de ifade edildiği üzere, dijital güvenlik risk yönetimi ile ilgili kamu politikası doğal olarak yatay ve sadece devlet yönetimi içinde değil, yerel, bölgesel ve uluslararası düzeyde tüm paydaşlarla işbirliği gerektiren niteliktedir. Bu, uzun süreli bir kamu politikası girişimidir.

Ancak, yol güvenliğinin aksine dijital ortamda paydaşların birbirine olan bağlılığı ve bağımlılığı oldukça yüksektir. Bu nedenle Sorumluluk İlkesi, paydaşların kararlarının başkaları üzerinde oluşturabileceği olası sonuçları da dikkate almaları gerektiğini vurgulamaktadır. Bu da şu maddelerle ilintilidir: i) İşledikleri kişisel verinin sahibi olan üçüncü taraflar, ii) Korumanın tüm paydaşların ortak çıkarı olan ve eylemlerinin ya da eylemsizliklerinin korunmasına ya da bozulmasına katkıda bulunduğu dijital ekosistemin tamamı[36]; iii) Dijital ortamın kritik altyapılar ve hizmetler için kullanılması nedeniyle tüm ekonominin ve toplumun bir bütün olarak işleyişi. En iyi uygulamaları benimsemek ve başkaların çıkarlarını da dikkate almanın ötesinde toplu sorumluluğu etkin olarak tesis etmenin başka yolları da mevcuttur: standartlara ve en iyi uygulamalara riayet etmek ve standart kuruluşlarına katılım sağlamak, sınırlar ve disiplinler arası da olmak üzere diğer paydaşlarla işbirliği içinde olmak vs.

Tüm paydaşlar, dijital güvenlik risk yönetiminde bulunurken aynı zamanda insan hakları ve temel değerleri dikkate almada (İlke 3) ve başkalarıyla işbirliği içinde olmada (İlke 4) sorumluluk almalıdır.

3. İnsan hakları ve temel değerler

Temel toplumsal kurallar dijital ortamda da geçerlidir. Bu nedenle insan hakları ve temel değerler dijital ortamda da geçerlidir ve bu ortamda korunmaları gerekmektedir. Bu haklar ve değerler çeşitli uluslararası belgeler tarafından bazen "öz değerler", "temel özgürlükler" vs. gibi isimlerle de ifade edilmektedirler. Bu alandaki önemli belgeler Evrensel İnsan Hakları Bildirgesi, Uluslararası Sivil ve Politik Haklar Sözleşmesi ve Uluslararası Ekonomik, Sosyal ve Kültürel Haklar Sözleşmesi'dir[37].

Nasıl kullanıldıklarına bağlı olarak dijital güvenlik riskini yönetmek üzere benimsenmiş olan güvenlik önlemleri[38]insan haklarını ve temel değerleri etkileyebilmekte ya da kısıtlayabilmektedir. Bunlar ifade özgürlüğünü, bilginin serbest dolaşımını, bilgi ve iletişimin gizliliğini, gizliliğin ve kişisel verilerin korunmasını, açıklığı ve adil yargılanmayı etkileyebilmektedir[39]. Örneğin güvenlik önlemleri gizlilik korumasını arttırabilmekte ya da kurumlardaki olumsuzluklar hakkında içerden bilgi verenler (whistle blower) ve insan hakları aktivistleri için anonimlik sağlayabilmektedir. Bunlar aynı zamanda vatandaşların hukuksuz bir şekilde izlenmesine ya da aktivistlerin sunduğu içeriğe erişimi engellemekte de kullanılabilmektedir. İlkede sayılmamış diğer hakları ve değerleri de etkileyebilmektedirler. Bu nedenle sorumluluk sahibi bir yaklaşım göstermek adına, dijital güvenlik risk yönetimi için alınan kararların bu haklar ve değerler üzerindeki sonuçları da dikkate alınması gerekmektedir.

Bu İlkeler tüm paydaşlar için geçerlidir. Kurumların insan hakları ve temel değerleri engelleyen dijital güvenlik önlemlerini benimsemenin imaj ve güvenilirlikleri üzerinde risk oluşturabileceğinin ve bunun hukuki sorumluluklarına girdiğinin farkında olmaları gerekmektedir. Güvenlik risk yönetimi kararlarının insan hakları ve temel değerler üzerinde

oluşturabileceği etkiyi değerlendirebilmek için dijital risk yönetimi döngüsünün sistematik yapısından faydalanmaları ve bu önlemleri uygun olacak şekilde ayarlamaları gerekmektedir. OECD Gizlilik Rehber Esasları tarafından çağrısında bulunulmuş olan gizlilik yönetimi programları uygulamalarının halihazırdaki risk yönetimi çerçevelerine ve idari yapılara eklemlenmeleri mutlaka fayda sağlayacaktır[40].

Dijital ortamı tasarlayan, işleten ya da yöneten paydaşlar (örneğin BİT uzmanları) BİT ürün ve hizmetlerinde dahil ettikleri güvenlik önlemlerinin insan haklarını kısıtlamada kullanılabilme olasılığını dikkate almalı ve buna göre hareket etmelidirler. Bazı durumlarda insan hakları üzerindeki potansiyel etkiler BİT ürün ve hizmetlerin kullanıldığı bağlama bağlı olup tasarım yoluyla bunların önlenmesi mümkün olmayabilmektedir. Bu gibi durumlarda BİT uzmanlarının bu ürün ve hizmetin kullanıcılarını potansiyel olumsuz etkileri ve bunu nasıl önleyebilecekleri konusunda bilgilendirmeleri gerekmektedir. Son olarak, hükümetler politikalarının dijital güvenlik risk yönetimini teşvik ettiğini ve bu alandaki uluslararası yükümlülüklerinin yanında hukuki ve düzenleyici çerçeveye uymasını sağlamalıdırlar (bkz. Bölüm 2. A. 2).

"Altın kural" olarak ya da etik karşılıklılık olarak adlandırılan ("insan başkalarına kendisine davranılmasını istediği şekilde davranmalıdır") ilkenin ifadesi olarak paydaşların aynı zamanda kendi eylemlerinin ya da eylemsizliklerinin başkalarına zarar verebileceğinin ve dijital ortamın kendisini de etkileyebileceğinin farkında olmaları gerekmektedir. Bununla beraber, etik bir şekilde davranmalı, yani başkalarının ve toplumun bir bütün olarak hukuki çıkarlarını gözetmelidirler. Etik davranış dijital ortamın açık, küresel ve birbirine bağlı yapısının paydaşların eylemlerinin yada eylemsizliklerinin etkisini arttırabildiği dikkate alındığında oldukça önem arz etmektedir.

Kurumların dijital güvenlik risk yönetimi uygulamaları ve prosedürlerinde genel bir şeffaflık politikasına sahip olmaları gerekmektedir. Ancak bu genel politikaların uygulanmasında kullanılan yöntemlerle ilgili rehber esaslar için olması gerekenden daha fazla şeffaflığın güvenliği zaafa uğratabildiğini gösteren durumlara özellikle dikkat çeken ve olası denetim mekanizmalarını da dikkate alan daha fazla çalışma gerekmektedir.

4. İşbirliği

Daha önce de vurgulandığı üzere dijital ortamın küresel anlamda birbiri ile bağlantılı olan yapısı paydaşlar arasında birbiri ile bağımlılık meydana getirmektedir. Birbiri ile bağımlı olma durumunun, paydaşların toplu haldeki gücüne dayalı olarak her biri için ekonomik ve sosyal fayda sağlamak gibi olumlu yönleri vardır. Ancak aynı zamanda karmaşıklığın artması, tehditlerin ve açıkların yayılmasını sağlaması ve potansiyel olarak toplu riskin artmasını sağlaması gibi çeşitli dezavantajları da mevcuttur. Paydaşlar hem kendi aralarında birbirine bağımlı hem de dijital ortama bağımlı oldukları için işbirliği esastır.

Dijital güvenlik risk yönetimi birçok yönüyle bir dereceye kadar işbirliği gerektirmektedir[41] ve izole bir paydaş tarafından başarılı bir şekilde ele alınamaz. Bu yüzden işbirliği Tavsiye Metnindeki diğer tüm İlkeler için zemin teşkil etmektedir. Örneğin: i) farkındalık ve beceriler, daha fazla farkındalığa ve beceriye sahip olanların, daha fazla farkındalık ve güç sahibi olma yolunda kendi çıkarlarını anlayabilmeleri gereken başkalarını bilgilendirmesini, eğitmesini ve yetiştirmesini gerektirmektedir; ii) sorumluluk tüm paydaşlar arasında rolleri, yetkinlikleri ve bağlama göre paylaşılmaktadır, böylelikle birbirini tamamlayan rollerdeki paydaşların bu

sorumluluklarının bütünsel bir şekilde üstlenebilmeleri için işbirliği gerekmektedir; iii) kuralları genellikle hukuk tarafından belirlenmiş olsa da insan hakları ve temel değerler etik terimler yoluyla ifade edilebilmekte ve tam olarak anlaşılabilmeleri ve dikkate alınabilmeleri için taraflar arasında diyalog ve tartışmaya gereksinim duymaktadır. İşbirliği aynı zamanda Uygulama İlkeleri için, uygulanmalarının ekonomik ve sosyal faaliyetleri yürütmekten sorumlu paydaşlar ile bu faaliyetlerin bağımlı olduğu dijital ortamı sağlamakla sorumlu paydaşlar arasında kapsamlı işbirliği gerektirmesi nedeniyle önem arz etmektedir. İşbirliği güvenlik önlemleri, inovasyon ve hazırlık önlemlerinin tam olarak uygulanmasının yanında insanların davranışlarını değiştirmelerini ve dijital güvenlik risk yönetimi için yönetim süreçlerinin benimsenmesini gerektiren teknik olmayan yönlerde de önem arz etmektedir.
Dijital güvenlik riskini daha iyi yönetebilmek adına yapılan işbirliğinin tüm paydaşları, üstlendikleri roller dikkate alınarak içermesi gerekmektedir. İşbirliği kurumlar içinde yapılmalı ve tüm sınırları aşmalıdır. En üst düzeydeki liderlik iç risk yönetim politikaları ve çerçevelerinin etkili işbirliği şartları sunmasında önemli rol oynamaktadır. Önemli bir olgu da, kurumların dijital ortamı ekonomik ve sosyal faaliyetleri için kullanan kısımları ("işletme tarafı") ile ortamı sağlayan kısımların ("BİT tarafı") ve hukuki ve düzenleyici uyumluluğu sağlayan kısımların hepsinin arasında bir işbirliği olmasıdır.

Aşağıda sıralandığı gibi, birçok farklı işbirliği türünden bahsedilebilmektedir:

- Kurumlar arasında, örneğin tehditlerin ve açıkların değer zinciri üzerindeki farklı şirketler ve ortaklar arasında olası yayılmasına müdahale etmek adına. Örneğin farklı bakanlıklar ve ajansların, farklı seviyedeki yönetimlerin (örneğin yerel/eyalet/ulusal) ve üstlenicilerin arasında da olduğu gibi benzer kaygılar devlet yönetimi içinde de güdülmektedir.

- Ortak tehditlerle karşı karşıya olan ve aynı ekonomik sektörde bulunan farklık kurumlar arasında. Bazı durumlarda, örneğin kritik altyapı hizmetlerinde hükümetler bu gibi işbirlikleri teşvik edebilmektedir.

- Kamu ve özel sektörler arasında, örneğin emniyet güçlerinin, eğitim kuruluşlarının ve daha genelde sivil toplumun özel sektörle işbirliği yapması gibi.

- Kurumlar ile kullanıcıları ve müşterileri, ve daha genel anlamda sivil toplum arasında yapılan işbirliği.

Kamu politikaları oluşturma bağlamında, daha iyi politikaların geliştirilmesi ve daha geniş katılım sağlanması için gerekli şartları oluşturmada çok paydaşlı yaklaşım oldukça önemli yer tutmaktadır (Bölüm 2. A. 4). Bu durum daha pratik seviyede, farkındalık ve beceriler, siber suç (örneğin emniyet güçleri ile işbirliği), BGVME/BAME[42], bilgi alışverişi ve paylaşımı[42] gibi birçok alanda kamu-özel sektör ortaklığı ve girişimlerine dönüşebilmektedir. Bölüm 2 (özellikle B. 3, B. 4 kısımları) kamu-özel sektör[44] işbirliği alanları ile ilgili birçok örnek sunmaktadır.

Son olarak uygun olduğu durumlarda işbirliği sınır ötesine de taşınmalıdır.

Uygulama İlkeleri

Tüm dijital güvenlik risk yönetimi döngüsü bu belgenin "Ana Kavramlar" kısmında ifade edilmiştir. Aşağıda sıralanan bileşenler her bir İlkeye odaklanmaktadır. Yine de genel bir mesele olarak dijital güvenlik risk yönetimini, faaliyetleri uygulamalarının sürekli değişen ve bu yüzden sürekli belirsizlik içinde olan bağlamına olabildiğince cevap verebilecek durumda tutmak yoluyla artan faydalar için fırsatlar oluşturabilen yaratıcı ve esnek karar alma süreçleri olarak anlayabilmek oldukça önem arz etmektedir. Bu, paydaşların başarı olasılıklarını arttırabilmeleri için esneklik ve uyum sağlayabilme yetisi kazandıran bir **dinamik bir zorluğa dinamik müdahale** yöntemidir. Bu yüzden dijital güvenlik risk yönetiminin yapısı aşağıda sıralandığı gibi olmalıdır:

- *Döngüsel:* ekonomik ve sosyal faaliyetler, onları barındıran dijital ortam ve dijital güvenlik riskleri sürekli olarak değişim içindedir. Buna ayak uydurmak, idealde dijital güvenlik riskinin sürekli olarak gözden geçirilmesini gerektirmektedir. Ancak pratikte faaliyetin yönlendirdiği genel bir döngünün yanında yeni tehditlerin ve açıkların ortaya çıkması, yeni vakaların meydana gelmesi, diğer bağlamsal olguların değişmesi gibi olayların yönlendirdiği daha özel döngülerin oluşturulması gerekmektedir. Risk yönetiminin döngüsel yapısı Şekil 1'de en alttan risk değerlendirme aşamasına ve faaliyetle ilgili inovasyon durumunda da tasarım aşamasına dönen oklar yardımıyla gösterilmektedir.

- *Bütüncül:* dijital ortamın birbiri ile bağlı olması nedeniyle risk yönetimi yaklaşımının da bütünsellik içinde olması gerekmektedir. Örneğin, değer zincirinin belli bir aşamasındaki açıkların zincirin başka bir aşamasından gelen tehdit tarafından istismar edilebilmesi ve üçüncü bir noktada sonuç doğurabilmesi nedeniyle risk yönetimi, ilgili faaliyetin tüm değer zincirini kapsamalıdır. Değer zinciri boyuncaki insanlarla (bireylerle), süreçlerle (kurallarla ve prosedürlerle) ve kullanılan teknolojilerle alakalı bileşenleri de kapsamalıdır. Bu yüzden yineleyen süreçler ya da metodolojiler oluşturmadan diğer risk kategorileri ile beraber yönetilmelidir.

- *Sistematik:* bütüncül bir risk yönetim döngüsünün karmaşıklığı ilgili kurumun ve faaliyetin karmaşıklığını yansıtma eğilimindedir. Bu artan karmaşıklığı yönetebilmek adına en doğru yol, farklı bileşenlerin ayrıldığı ve her birine bütünün bağlamında müdahale edildiği sistematik bir yaklaşımdır.

Döngüsel, bütüncül ve sistematik bir dijital güvenlik risk yönetimi yaklaşımının oluşturulması, aşağıda (İnovasyon İlkesi) anlatıldığı gibi riskin fırsatlarla beraber yönetildiği koşulları ortaya çıkarmaktadır. Bu aynı zamanda insan haklarını ve temel değerleri, başkalarının hukuki çıkarlarını gözetmenin yanında güvenlik önlemlerinin insan hakları ve temel değerler ve dijital ortam üstündeki potansiyel etkilerini dikkate almada daha kapsamlı ve uygun bir yaklaşım sunmaktadır.

Çeşitli metodolojiler, standartlar ve en iyi uygulamalar risk yönetiminin yürütülmesine destek olabilmektedir. Bunlar tüm sürecin yanında güvenlik önlemleri ve hazırlık gibi daha özel yönler için de olmak üzere tüm seviyelerde yardımcı olmaktadır.

5. Risk değerlendirme ve müdahale döngüsü

Sürekli bir risk değerlendirme ve müdahalesi güvenlik ile ilgili kararların ilgili sosyal ve ekonomik faaliyetle ve risk ile uygun ve orantılı olmasını sağlamak adına önemlidir.

Risk değerlendirmesi çeşitli alt aşamalara ayrılabilen *analitik bir süreçtir*. Buna göre risk i) tespit edilir: yani risk faktörleri genelde deneyime, tarihsel verilere, teorik analize, uzmanların görüşlerine ve fikirlerine vs. dayalı olarak tanınır; ii) analiz edilir: yani risk anlaşılır ve riskin seviyesi belirlenir. Yukarıda da bahsedildiği üzere bu seviye genelde olasılık ve ilgili sosyal ve ekonomik faaliyet üzerindeki etki üzerinden ifade edilir; iii) değerlendirilir: yani risk, faaliyet ve ondan beklenen sosyal ve ekonomik hedefler ve faydalar ile ilgili kabul edilebilir risk seviyesi ile karşılaştırılır.

Her ne kadar risk değerlendirmesi öncelikle hedeflerin üzerindeki belirsizliğin potansiyel sonuçlarına odaklanması gerekiyor olsa da uygun olduğu durumlarda, üstlendikleri rollerin kapsamına ya da riskten etkilenme durumlarına göre başkaların üzerindeki potansiyel etki de dikkate alınmalıdır (örneğin gizlilik, bkz. Kutu 4). Risk değerlendirmesinin aynı zamanda tüm dijital ekosistemdeki belirsizliğin (toplu risk) olası etkilerini de dikkate alması gerekmektedir.

Risk müdahalesi[45], *bir karar alma süreci* olup, risk değerlendirmesinin sonucuna bağlı olarak onu nasıl değiştirip faaliyetten beklenen ekonomik ve sosyal faydalara göre kabul edilebilir seviyeye getirebilineceği ile ilgilidir ve aynı zamanda başkalarının hukuki çıkarları üzerindeki olası etkileri de ("kabul edilebilir risk seviyesi") dikkate almaktadır. Bu hukuki çıkarlar insan hakları ve temel değerlerin (İlke 3) yanında dijital ortamın işleyişini de kapsamaktadır.

Genel olarak riske müdahalede dört olasılık vardır (bkz. Şekil 1), bunlar şu şekilde sıralanabilir:

- *Kabul etmek*: "riski almak" ve belirsizliğin kısmi ve tamamen başarısızlık da dahil olmak üzere hedefler üzerindeki etkilerini kabul etmek. Eğer faaliyet üstlenildiyse risk tamamen elimine edilemez, bu yüzden belli bir "artık" risk kabul edilmelidir (bkz. İlke 2 Sorumluluk). Genelde risk yönetimi,faaliyetin yürütülmesinden elde edilen faydanın artık riskten ağır basmasıyla ekonomik olarak verimli olur.

- *Şu yöntemler vasıtası ile kabul edilebilir seviyeye indirmek*: i) risk yönetiminde tespit edilmiş olan açıkları istismar eden belli potansiyel tehditlere karşı faaliyetleri korumak için güvenlik önlemleri seçmek ve uygulamak (İlke 6); ii) inovasyona (İlke 7) yol açabilecek bir şekilde, örneğin tekrar tasarlamak ya da farklı bir şekilde yürütmek vasıtasıyla faaliyeti değiştirmek; iii) vakaların gerçekleşmesi halinde bunlarla başa çıkabilmek için hazırlık önlemleri tanımlamak ve gerektiğinde uygulamak (İlke 8).

- *Transfer etmek*: örneğin sigorta gibi sözleşmeler vasıtasıyla faaliyetin hedefi üzerindeki istenmeyen etkileri başka birine yöneltmek. Dijital güvenlik risk sigortası ileri çalışmalar için faydalı bir alan olabilecek durumdadır.

- *Kaçınmak*: faaliyeti gerçekleştirmeyerek ya da ilgili dijital bileşeni ortadan kaldırarak riski elimine etmek.

"Kabul edilebilir risk seviyesi", faaliyeti gerçekleştiren ve risk ile karşı karşıya olan paydaş tarafından belirlenmelidir. Paydaşın bir faaliyeti üstlenirken kabul etmeye razı olduğu risk

miktarının ölçütüne “risk iştahı” adı verilmektedir. Bu faaliyet ve hedefleri ile ilgili birçok faktörün yanında kurum kültürü ve stiline, piyasa koşullarına ve teknik ortama vs. bağlıdır. Bazı durumlarda hukuki ve düzenleyici bağlama göre de sınırlandırılabilmektedir. Tamamen kabul edildiği ya da tamamen kaçınıldığı durumlar haricinde riskin nasıl kabul edilebilir bir seviyeye indirileceği ya da transfer edileceği yönünde bir karar alınması gerekmektedir.

6. Güvenlik önlemleri

Güvenlik önlemleri, ekonomik ve sosyal faaliyetlerin korunmasında vazgeçilmez olduğu kadar bu faaliyetler üstünde olumsuz etkilerde de bulunabilmektedir. Bu ilke güvenlik önlemlerinin riske ve ilgili ekonomik ve sosyal faaliyete uygun ve orantılı olarak en iyi şekilde risk değerlendirme ve müdahale sürecine dayanarak seçilmesini, uygulanmasını ve geliştirilmesinin yollarını vurgulamaktadır (dijital güvenlik risk yönetimi tanımı için önceki kısımlara bakınız).

Örneğin, güvenlik önlemleri faaliyetin maliyetini arttırabilir ve kullanılabilirliğini, performansını ve iyileştirilme potansiyelini etkileyebilir. Birçok teknik güvenlik önlemi bir düzeye kadar bilgi akışının kısıtlanmasını (örneğin güvenlik duvarı) ya da prosedürlere ek basamaklar getirilmesini (örneğin doğrulama) içermektedir. Bazıları karmaşıklığı arttırmakta (örneğin kriptografi) ve yönetilebilir halde bırakabilmek için işlevsellik yönünden bir takım ödünler vermeyi gerektirmektedir. Potansiyel olarak insan haklarını ve temel değerleri etkileyebilecek olan güvenlik önlemlerine güvenlik tehditlerini tespit edebilmek için trafik akışını izleme ve analiz etme (“derin paket denetimi”) gibi kişisel verilere erişim gerektiren yöntemler örnek olarak gösterilebilir. Güvenlik uzmanları genelde işleri esnasında kişisel verilerle karşı karşıya bulunmaktadır. Örneğin, bir vakayı analiz etmek için kişisel hesaplara erişmeleri gerekebilmektedir. Aynı zamanda bir vakayı daha iyi analiz edebilmek ya da adli tıp soruşturmaları için vakayla ilgili kişisel verileri üçüncü taraflara aktarmaları söz konusu olabilmektedir. Kriz yönetimi de, örneğin bir tehditin yayılmasını önlemek için bir hizmeti kaldırmak ve potansiyel olarak kullanıcıların haklarını sınırlamak gibi durumların oluşmasına neden olabilmektedir. Dijital güvenlik risk yönetim döngüsü, güvenlik önlemlerinin bu gibi potansiyel olumsuz etkilerinin dikkate alınması ve uygun araçlar ve uygulamalarla giderilmesini sağlamak adına sistematik bir yaklaşım sunmaktadır.
Güvenlik önlemleri bazen “güvenlik mekanizmaları”, “güvenlik kontrolleri” ya da “güvenlik tedbirleri” olarak da adlandırılmakta ve farklı yapılara sahip olabilmektedir: dijital (örneğin güvenlik yazılımı), fiziksel (örneğin kilitler, kameralar, çitler) ya da karma (örneğin akıllı kart); insanlarla ilgili (örneğin eğitim), süreçlerle ilgili (örneğin kurumsal kural ya da uygulamalar) ya da teknolojiler ile ilgili (örneğin kriptografi); hukuki (örneğin sözleşme), yöntemsel (örneğin standartlar), yönetimsel vs. Bunlar sadece olası sınıflandırmalar örnektir.

Güvenlik önlemleri aynı zamanda açıklara da hitap etmektedir. Tıpkı tehditlerin sürekli değişmesi gibi, dijital ortamdaki açıklar da sürekli olarak değişmektedir. Bu nedenle kurumlar sürekli olarak yeni ortaya çıkan tehditlerin önüne geçebilmek için açıkları olabildiğince çabuk taramalı, değerlendirmeli ve uygun bir şekilde müdahale etmelidir.

Riskin dinamik bir yapısı olması nedeniyle güvenlik önlemleri faaliyet planlanırken yukarıda açıklanmış olan döngüsel, bütüncül ve sistematik yaklaşım kullanılarak belirlenmeli ve faaliyet süresi boyunca güncellenmelidir. Bazı önlemler faaliyete tasarım aşamasında yani örneğin önemli olmaları ya da faaliyetin ilgili kısmının sonradan değiştirilmesinin mümkün olmaması gibi nedenlerle temel bileşen olarak yerleştirilmelidir. Ancak, risk dinamik

olduğundan diğer güvenlik önlemleri de sürekli risk değerlendirme ve yönetim döngüsü çerçevesinde ele alınmalıdır.

Dijital ortamın tasarımı, yönetimi ve işletiminde role sahip olan paydaşlar, güvenlik önlemleri ile ilgili olarak her zaman en iyi uygulamaları benimsemeli ve standartlara uymalıdırlar. Çoğu genel ve sektör tabanlı standartlar ve iyi uygulamalar güvenlik önlemlerine uygulanabilmektedir. Bu gibi standartlara uymak genelde güvenlik risk yönetiminin yaygın meselelerine hitap edebilmekte ve kuruma ya da faaliyete özel meselelere daha fazla zaman ve kaynak ayrılabilmesine olanak tanımaktadır.

BİT ürün ve hizmeti geliştiren ve idare eden paydaşlar bu ürün ve hizmetlere güvenlik önlemleri yerleştirmeli, kullanıcılarını bilgilendirmeli ve uygun olan durumlarda bunların kullanımı ile ilgili oluşan risklerle baş edebilmeleri için destek sağlamalıdır.

7. İnovasyon

Güvenlik önlemlerini uygulamanın yanında paydaşlar dijital güvenlik riskine maruziyetlerini faaliyetler ve güvenlik önlemleri ile ilgili inovasyonlar yoluyla da azaltabilmektelerdir. İnovasyon genelde yeni ya da önemli ölçüde geliştirilmiş bir ürünün (mal ya da hizmet) ya da sürecin (üretim ya da dağıtım yöntemleri), yeni bir pazarlama yönteminin ya da iş uygulamaları, işyeri organizasyonu ya da dış ilişkiler alanlarında yeni bir kurumsal yöntemin uygulamaya sokulması olarak tanımlanmaktadır[46].

Dijital güvenlik risk yönetimi bağlamında, riski azaltmak adına yapılan inovasyon dijital boyutları da bulabilen ya da bulanmayabilen birçok farklı şekilde olabilmektedir. Örneğin, kurumun ekonomik ya da iş modelini, ödeme yöntemleri gibi süreçleri ve hatta ürünün fiziksel, hukuki ya da diğer dijital olmayan bileşenlerinin tasarlanmasını etkileyebilmektedir. Bir faaliyetteki belirsizliğin olası etkilerini azaltmak için uygulanan inovasyonun kendisi de faaliyetin başka boyutları ile ilgili belirsizliklere neden olabilmektedir. Bu nedenle tekrar bir değerlendirme ve müdahale döngüsüne sokulması gerekmektedir.

Böylelikle, dijital güvenlik risk yönetimi, bir faaliyetle ilgili ekonomik ve sosyal karar alma süreçlerinin bir parçası olarak yaklaşıldığında inovasyon için itici bir güç olabilmektedir. Dijital güvenlik risk yönetimi kararları temel ekonomik ve sosyal karar alma sürecinden izole edildiğinde bunlara inovasyon için potansiyel itici güç olarak yaklaşılması daha zor hale gelmektedir. Bu durumlarda bu kararlar, rekabet avantajı sağlamada teşvik edici olmaktan ziyade yavaşlatıcı olarak ya da maruz kalınan sınırlamalar olarak görülebilmektedir.

Aslında risk, inovasyon ve ekonomik ve sosyal gelişme birbirleriyle oldukça ilintilidir. Örneğin tarih boyunca yapılan birçok insan icadı ve gelişmeyi belirsizlikle baş edebilme arzusu ya da gereksinimi ile ilişkili olarak görmek mümkündür: örneğin iklim belirsizlikleri mutlak surette şemsiyenin icadının yanında kıtlık riskini azaltabilmek adına tarım, gıda depolama, işleme ve dağıtımı gibi alanlarda da hatırı sayılır gelişmelere neden olmuştur. Dijital ortamda risk ve inovasyonun birbiriyle ilişkisini daha iyi anlayabilmek adına daha fazla çalışma yapılması faydalı olacaktır.

Bu açıdan bakıldığında, bu İlke daha geniş bir biçimde risk yönetiminin değer koruma ve üretmede genel bir yaklaşım olarak görülebildiğinin kabul edilmesi olarak yorumlanabilmektedir. Risk yönetimi, kurumların sürekli değişen bir ortamda başarı olasılıklarını arttırabilmek adına belirsizliklere sistematik olarak müdahale edebilmesini

sağlamaktadır. Ancak, yukarıda da belirtildiği gibi, belirsizliklerin faaliyete etkileri her zaman olumsuz olmayabilir. Riskin hem olumlu hem de olumsuz tarafı vardır: belirsizlikler bir faaliyeti olumsuz olarak etkileyebildikleri gibi aynı zamanda faaliyeti iyileştirebilecek fırsatlar da oluşturabilmektedir. Riski ve fırsatları aynı karar alma sürecinin her iki yüzünü de oluşturduğu düşünüldüğünde, risk yönetimi şu maddeleri kapsayan bir döngü olarak ele alınabilir: i) "olumsuz risk", "olumlu risk" (fırsatlar) ile beraber değerlendirilir; ve ii) risk müdahalesi, hedefleri en iyi şekilde yerine getirebilmek adına olumsuz riski kabul edilebilir seviyelere indirebilmenin *yanında* pozitif riskten de faydalanmayı, yani fırsattan yararlanmayı içermektedir. Bu iki olgunun tek bir döngüsel, bütüncül ve sistematik çerçevede birleştirilmesi kurumun çevikliğini ve müdahale edebilirliğini arttırmanın yanında rekabeti desteklemekte ve inovasyonu sağlamaktadır.

Risk yönetimine bu türden bir yaklaşım nispeten yenidir[47] ve potansiyel faydalarının ve genelleştirilmesindeki engellerin özellikle dijital güvenlik riski ile ilgili olacak şekilde daha iyi anlaşılması için daha fazla çalışma yapılması gerekmektedir. Bu nedenle Tavsiye Metni, riske yaklaşımda risk faktörlerini açıklamakta kullanılan terimlerle (örneğin tehditler, açıklar ve vakalar) ve koruma alanı ile ilgili olan "güvenlik" kavramına ait terminolojiyle (örneğin süreklilik, bütünsellik, gizlilik) gösterildiği üzere olumsuz yönlerini ele almaktadır. Yine de İnovasyon İlkesi dijital güvenlik risk yönetiminin fırsatları değerlendirmede ve inovasyona destek olmada öncü bir güç olarak görülebileceğinin altını çizmektedir.

8. Hazırlık ve süreklilik

Dijital güvenlik risk yönetimi, vakaların her zaman önlenebildiği tamamen "güvenli ve korunaklı" bir dijital ortam sağlamanın imkansız olduğunu kabul etmeye dayanmaktadır. Sağlam güvenlik önlemlerinin uygulanmasına ve düzgün bir şekilde yönetilmesine rağmen vakalar meydana gelebilir ve ekonomik ve sosyal faaliyetleri etkileyebilirler. Bu nedenle dijital güvenlik risk yönetimi güvenlik önlemlerinin ve inovasyonun oluşturulmasından ibaret değildir. Aynı zamanda, vakalar meydana geldiğinde onların ekonomik ve sosyal faaliyetler üzerindeki olumsuz etkilerini azaltmak ve bu faaliyetlerin devamlılığını ve dayanıklılığını sağlamak adına risklerin azaltılmasını sağlayacak mekanizmaların önceden tanımlandığı hazırlık ve süreklilik planlarını da içermesi gerekmektedir.

Bir hazırlık ve süreklilik planının vakaların dijital ortamda yayılma ve tırmanma hızlarını dikkate alması gerekmektedir. Vakanın tırmanma aşamaları genellikle ilgili ekonomik ve sosyal faaliyetleri ve hedefleri etkileyen sonuçların kapsamı ve büyüklüğü ile alakalı olarak ayırt edilmektedir. İkaz (etki yok), Vaka (sadece IT üzerinde etki var), Acil Durum (sınırlı ekonomik ve sosyal etki), Kriz (kurumun varlığını tehdit edecek düzeyde etki var) gibi çeşitli tırmanma seviyeleri tanımlanabilmektedir. Bağlama göre başka terimler ve seviyeler de kullanılabilir. Örneğin, kamu politikaları tek bir kuruma, bulunduğu sektöre, ulusal ekonominin bütününe ve ulusal sınırların ötesine olan etkileri dikkate alabilmektedir. Vaka esnasında riskin uygun bir şekilde yönetilebilmesini sağlama için her bir tırmanma seviyesi için sorumluluk dağılımı farklı şekilde olmalıdır. Burada, bir vakanın ekonomik ve sosyal etkilerinin yanında teknik boyutlarının da karar alıcılar tarafından anlaşılmasını sağlamak için işbirliği yine önemli bir rol üstlenmektedir.

Bir hazırlık planının dijital güvenlik vakalarında önleme, tespit etme, müdahale ve toparlanma aşamalarını kapsaması gerekmektedir. Aynı zamanda hem bireysel hem de kamu ve özel

sektör kurumları arasında ve ulusal sınırların ötesinde de olmak üzere diğer paydaşlarla uygun bilgi alış verişi gibi işbirliğine yönelik eylemleri hesaba katmalıdır. Riskin dinamik yapısını da dikkate almak adına sürekli ve döngüsel bir biçimde test edilmeli, değerlendirilmeli ve gözden geçirilmelidir. Aynı zamanda Bilgisayar Acil Müdahale Ekipleri (BAMEler) olarak da adlandırılan Bilgisayar Güvenlik Vakası Müdahale Ekipleri (BGVMEler) paydaşlara belli dijital güvenlik vakalarına karşı müdahale etmeye yardımcı olmak anlamında önemli role sahiptir. Karar alıcılar BGVMEler/BAMElerin faaliyetlerini yansıtan uluslararası olarak karşılaştırılabilir istatistiksel göstergelerden genel risk seviyesini daha iyi anlayabilmek adına yararlanabilir.

Son olarak, uygun bildiri prosedürleri de planın uygulanmasının önemli bir parçası olarak görülmelidir. Bunlar bazı durumlarda gönüllü olarak, bazı durumlarda da kanunla belirlenmiş olarak düzenlenebilmektedir.

Ek Gelecekteki çalışmalar için olası alanlar

Gelecek çalışmalar için olası alanlar şunları kapsamaktadır:

- Kurumlarda dijital güvenlik risk yönetim idaresi: teknik bir meseleden liderlik önceliğine
- Gizlilik için risk yönetimi: OECD Gizlilik Ana Esaslarını daha iyi uygulayabilmek için dijital güvenlik risk yönteminden yararlanmak. Dijital güvenlik ve gizlilik risk yönetimleri arasındaki benzerlikler, farklılıklar ve sinerjileri ve ortak bir çerçeveden oluşabilecek fırsatları incelemek
- İnovasyon ve dijital güvenlik risk yönetimi arasındaki ilişkinin yanı sıra dijital güvenlik meselelerine "risk ve fırsat" yönetimi yaklaşımı uygulandığı durumda (değer korumak ve üretmek için risk yönetimi) ortaya çıkan uygulanabilirlik, faydalar ve güçlükler.
- Dijital güvenlik risk yönetimi sigortacılığının getireceği fırsatlar ve güçlükler.
- İlkeleri KOBİler ve bireyler için yorumlamak.
- Dijital güvenlik risk yönetimi ile ilgili denetim.
- Tavsiye Metninde Bölüm 2'de geçen kamu politikaları için rehberlik
- Uluslararası işbirliği ve gelişmekte olan ekonomiler.
- Dijital güvenlik riskine dair bulguları geliştirmek.

Kaynakça

ACMA (Australian Communications and Media Authority) (2011), *An overview of internationalcyber-security awareness raising and educational initiatives*, www.acma.gov.au/theACMA/an-overview-of-international-cyber-securityawareness-raising-and-educational-initiatives.

Angwin, J. (2015), *The World'sEmail Encryption Software Relies on One Guy,Who is Going Broke*, www.propublica.org/article/the-worlds-email-encryptionsoftware-relies-on-one-guy-who-is-going-broke.

App Promo (2012), "Wake Up Call – If You Spend It, They Will Come", http://app-promo.com/wake-up-call-infographic/ (erişim tarihi 25 Ağustos 2015).

App Promo (2013), "App Promo White Paper. Slow and steady win the race. App Developers That Stick it Out Come Out on Top", App Promo Developer Survey, June 2013, http://app-promo.com/wp-content/uploads/2013/06/SlowSteady-AppPromo-WhitePaper2013.pdf (erişim tarihi 25 Ağustos 2015).

Ashford W. (2013), *Targeted cyber espionage on the increase, McAfee warns*, www.computerweekly.com/news/2240185167/Targeted-cyber-espionage-onthe-increase-McAfee-warns. Aven, T. (2012), "The risk concept - historical and recent development trends", in *ReliabilityEngineering&SystemSafety*, Volume 99, March 2012, pp. 33–44, http://dx.doi.org/10.1016/j.ress.2011.11.006.

CBC News (2012), "Nortel collapse linked toChinese hackers", www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591(erişim tarihi 25 Ağustos 2015).

Choe, S. (2014), "Theft of Data Fuels Worries in South Korea", New York Times, www.nytimes.com/2014/01/21/business/international/theft-of-datafuels-worries-in-south-korea.html (erişim tarihi 25 Ağustos 2015).

CIGI (Centre for International Governance Innovation) (2014), *CIGI-Ipsos Global Survey on Internet Security and Trust*, https://www.cigionline.org/internetsurvey(erişim tarihi 25 Ağustos 2015).

CNIL (Commission Nationale de l'Informatique et desLibertés) (2012), *Methodology for privacy risk management*, www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf.

Council of Europe (2001), *Convention on Cybercrime*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Dark Reading (2012), "4 Long-Term Hacks That Rocked 2012", www.darkreading.com/application-security/database-security/4-long-term-hacksthat-rocked-2012/d/d-id/1138643 (erişim tarihi 25 Ağustos 2015).

ENISA (European Union Agency for Network and Information Security) (2013), *National Cyber Security Strategies in the World*, www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/
national-cyber-security-strategies-in-the-world(erişim tarihi 25 Ağustos 2015).

ENISA (n.d.), "Existing Taxonomies", www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies
(erişim tarihi 25 Ağustos 2015).

Europol (2013), *Notorious Botnet Infecting 2 Million Computers Disrupted*, www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computersdisrupted-0
(erişim tarihi 25 Ağustos 2015).

Fechner, B. (2014), *Lesentreprisesfrançaisesfaceaudéfi de l'espionnageindustriel*, http://lexpansion.lexpress.fr/actualite-economique/les-entreprisesfrancaises-peuvent-elles-relever-le-defi-de-l-espionnage-industriel_1633978.
html(erişim tarihi 25 Ağustos 2015).

Gaudiosi, J. (2014), "Why Sony didn't learn from its 2011 hack", http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/ (erişim tarihi 25 Ağustos 2015).

ISOC (Internet Society) (2015), *Collaborative Security: An approach to tackling Internet Security issues*, www.internetsociety.org/collaborativesecurity

Jackson, W. (2014), "Cyber Espionage Incidents Triple: Verizon Report", www.informationweek.com/government/cybersecurity/cyber-espionage-incidentstriple-verizon-report/d/d-id/1204612 (erişim tarihi 25 Ağustos 2015).

Kim, Y. (2014), "Top executives resign over massive data leak", www.koreaherald.com/view.php?ud=20140120001002(erişim tarihi 25 Ağustos 2015).

Kitten, T. (2014), "Chase's Cybersecurity Budget to Double", www.bankinfosecurity.com/chases-cybersecurity-budget-to-double-a-7427(erişim tarihi 25 Ağustos 2015).

Lee, R., M. Assante, M. and T. Conway (2014), *German Steel MillCyber Attack*, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Leyden, J. (2013), "Biggest DDoS attack in history hammers Spamhaus", www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood (erişim tarihi 25 Ağustos 2015).

Molla, R. (2012), "Most app developers make less than $500 a month", https://gigaom.com/2012/10/04/most-app-developers-make-less-than-500-amonth-chart/
(erişim tarihi 25 Ağustos 2015).

NACD (National Association of Corporate Directors) (2014), *NACD Reports Directors Dissatisfied with Cyber and IT Risk Information*,

www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=12530 (erişim tarihi 25 Ağustos 2015).

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST (National Institute of Standards and Technology) (2012), *Guide for conducting risk assessment. Special publication 800-30, revision 1*, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

O'Connor, C. (2014), "Target CEO Gregg Steinhafel Resigns in Data Breach Fallout", www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-greggsteinhafel-resigns-in-wake-of-data-breach-fallout (erişim tarihi 25 Ağustos 2015).

OECD (Organisation for Economic Co-operation and Development) (2002),*Recommendation of the Counci lConcerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security*, www.oecd.org/internet/ieconomy/15582260.pdf.

OECD/Eurostat (2005), *Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd Edition, The Measurement of Scientific and Technological Activities*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264013100-en.

OECD (2008), *Recommendation of theCouncil on the Protection of Critical Information Infrastructures*, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117.

OECD (2011), *Recommendation of the Council on Principles for Internet Policy Making*, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=270&InstrumentPID=275.

OECD (2012a), *Connected Minds: Technology and Today'sLearners,Educational Research and Innovation*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264111011-en.

OECD (2012b), "ICT Applications for the Smart Grid: Opportunities and Policy Implications", *OECD Digital Economy Papers*, No. 190, OECD Publishing,Paris, http://dx.doi.org/10.1787/5k9h2q8v9bln-en.

OECD (2012c), "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online", *OECD Digital Economy Papers*, No. 214, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k4dq3rkb19n-en.

OECD (2012d), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

OECD (2013a), *ICTs and the Health Sector: Towards Smarter Health and Wellness Models*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264202863-en.

OECD (2013b), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en&Book=False.

OECD (2014), *Recommendation on Digital Government Strategies*, www.oecd.org/gov/public-innovation/recommendation-on-digital-government-strategies.htm.

OSCE (Organisation for Security and Cooperation in Europe) (2013), *Decision no. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, www.osce.org/pc/109168.

Peters, S. (2014), "Pharmaceuticals, Not Energy, May Have Been True Target of Dragonfly, Energetic Bear", www.darkreading.com/pharmaceuticalsnot-energy-may-have-been-true-target-of-dragonfly-energetic-bear/d/did/1316869 (erişim tarihi 25 Ağustos 2015).

Piper, A. (2014), "Risk-informed innovation. Harnessing risk management in the service of innovation", www.economistinsights.com/technologyinnovation/analysis/risk-informed-innovation (erişim tarihi 25 Ağustos 2015).

Prince, B. (2014), "Incident Response Plans Lacking in Many Organizations: Survey", www.securityweek.com/incident-response-plans-lacking-manyorganizations-survey (erişim tarihi 25 Ağustos 2015).

Rawlinson, K. (2015), "Charlie Hebdo: 'Islamist cyber attacks' hit France",www.bbc.com/news/technology-30850702(erişim tarihi 25 Ağustos 2015).

SecurEnvoy (2012), "The RSA Security breach – 12 months down the technology turnpike", www.securenvoy.com/blog/2012/04/27/the-rsa-securitybreach-12-months-down-the-technology-turnpike/ (erişim tarihi 25 Ağustos 2015).

United Nations (1948), *Universal Declaration of Human Rights*, www.un.org/en/documents/udhr/.

United Nations (1966a), *International Covenant on Civil and Political Rights*, www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

United Nations (1966b), *International Covenant on Economic, Social and Cultural Rights*, www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx.

United Nations (2003), *Creation of a global culture of cybersecurity, Resolution adopted by the General Assembly A/RES/57/239*, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239.

United Nations (2013), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in theContext of International Security*, www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

Westby, J. (2012), *Governance of Enterprise Security: CyLab 2012 Report. How Boards & Senior Executives Are Managing CyberRisks*, http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf.

Yadron, D. (2014), "Internet Security Relies on Very Few", www.wsj.com/news/articles/SB10001424052702303873604579495362672447986 (erişim tarihi 25 Ağustos 2015).

Notlar

1. Enerji gibi, bkz. OECD, 2012b, ulaşım, imalat, vs.

2. Bkz. OECD, 2013a.

3. Bkz. OECD, 2012a.

4. Bkz. www.oecd.org/about/whodoeswhat.

5. Bkz. www.oecd.org/sti/ieconomy.

6. Bkz. www.oecd.org/legal/legal-instruments.htm.

7. Sırasıyla OECD Sanayi ve İş Dünyası İstişare Komitesi (BIAC), Sivil Toplum ve Bilgi Toplumu İstişare Komitesi (CSISAC) ve İnternet Teknik İstişare Komitesi (ITAC) tarafından temsil edilmektedir.

8. Örneğin bu Tavsiye Metninin öncülü (2002 Güvenlik Ana Esasları) ISO 27001:2002'da kaynak olarak gösterilmiş ve Birleşmiş Milletler Tasarısı 57/239 için ilham kaynağı olmuştur (United Nations, 2003).

9. Avrupa Konseyi, 2001. Aynı zamanda bkz. Avrupa Konseyi Siber Suçlar Programları Ofisi (C-PROC)www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.

10. Bkz. www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

11. Örnek olarak bkz. United Nations, 2013.

12. Bkz. OSCE, 2013.

13. Özellikle Telekomünikasyon ve Bilgi Çalışma Grubu (APEC TEL) vasıtasıyla.

14. Örneğin yerel, bölgesel, eyalet bazlı, federal vs. "Paydaşlar ve rolleri" kısmındaki açıklamalara bakınız.

15. Roller, yetkinlikler ve bağlam için Yardımcı El Kitabındaki "İlkelerin Uygulanabilirliği" kısmına bakınız.

16. CNIL, 2012, p. 13.

17. Ashford, 2013; Feshner, 2014; and Jackson, 2014.

18. Örnek olarak ABD Ticaret Odası, Nortel, Coca-Cola ve Japonya Maliye Bakanlığı'na yapılan uzun süreli saldırılar ile ilgili örnekler sunan Dark Reading, 2012. Nortel'in iflası, açıklandığı üzere dijital casuslu ve özellikle de şirketin bilgi işlem sistemine yapılan on yıllık gizli sızma ile ilintilidir. Bkz. CBC News, 2012.

19. Örnek olarak bkz. Europol, 2013.

20. Bkz. OECD, 2012d, ve ENISA, 2013.

21. 2012 yılında Forbes Global 2000 şirketlerinin 108'inin katılımı ile yapılan bir araştırma, katılımcıların %57'sinin gizli ve özel verilerin çalınması ve güvenlik ihlalleri ile alakalı itibar ve finans risklerini yönetmelerine yardımcı olabilecek siber sigorta kapsamının yeterliliğini analiz etmediği ya da siber risk yönetimi ile ilgili önemli faaliyetleri üstlenmediği ortaya çıkmıştır. Westby, 2012. Aynı zamanda bkz. NACD, 2014 ve Prince, 2014.

22. CIGI, 2014: kullanıcıların %78'i kişisel banka hesaplarına izinsiz girişlerden kaygı duymaktadır. Kullanıcıların %77'si birilerinin İnternet hesaplarına izinsiz erişmesi ve kişisel verilerini çalması konusunda kaygı duymaktadır. Kullanıcıların %72'si ülkelerindeki kurumlara yabancı ülkeler ya da terörist gruplar tarafından siber saldırı yapılması konusunda kaygı duymaktadır.

23. Burada, fikri mülkiyet bir güvenlik vakası (örneğin bir kurumun bilgi sistemine girilip gizli endüstriyel veya ticari sırların çalınması ya da bir internet sitesi değiştirilerek yasal olmayan içeriğin açıklanması (örneğin nefret suçu)) sonucu ortaya çıktığında bir kesişim olmaktadır.

24. Örneğin, "yoldan karşıya geçersen, bir arabanın çarpma riski vardır" önermesindeki risk bir olaya ya da vakaya işaret etmektedir; "arabalar karşıdan karşıya geçen yayalar için risk oluşturmaktadır" önermesinde ise risk bir tehdit ya da tehlikeye işaret etmektedir; ve "eğer karşıdan karşıya geçerken dikkatli olmazsanız ölme riskiniz vardır" önermesinde ise risk vakanın sonucuna işaret etmektedir.

25. Çeşitli ulusal, bölgesel ve uluslararası kurumdan, devlete ait ya da devletten bağımsız, genel ya da sektörel (örneğin finans, kamu yönetimi vs.) yaklaşımlardan ortaya çıkan birçok risk temelli standartlar ve metodolojiler mevcuttur. Örneğin Ağ ve Bilgi Güvenliği için Avrupa Birliği Ajansı (ENISA) bunlardan 17 tanesini http://rm-inv.enisa.europa.eu/methods adresinde sıralamaktadır. Bunun yanında risk değerlendirmesi yapmak için ABDNIST 800-30 Rev. 1 Rehberi (NIST, 2012) ve daha da güncel olarak Siber Güvenlik çerçevesi (NIST, 2014) gibi örnekler de mevcuttur. Standartlar genellikle Tavsiye Metni ile çelişmeden farklı bakış açılarını yansıtmakta, farklı kitlelere hitap etmekte, farklı terimler ve tanımlar kullanmaktadır. Örneğin "risk müdahalesi" terimi bazı standartlarda "riskin hafifletilmesi" olarak, bazılarında "riskin azaltılması" terimi "riskin hafifletilmesi" olarak, "riskin önlenmesi" terimi "riskin yok edilmesi" olarak ve "açıklar" terimi "zafiyet" olarak vs. geçebilmektedir.

26. "BİT uzmanları" büyük sayıdaki uygulama geliştiricileri de dahil olmak üzere ana meslekleri BİT uygulaması olmayan paydaşları da kapsayabilmektedir.

27. Bazı durumlarda bir meselenin teknik karmaşıklığının sonucu olarak dijital güvenlik riskinin düşürülmesi mümkün olmakla beraber bu bireylere bunu kontrol edecek gücü vermeden de yapılabilmektedir. Örneğin ağ hizmetleri ve diğer uzaktan verilen hizmetler güvenlik çözümlerini merkezi olarak sunmaktadır.

28. SecurEnvoy, 2012.

29. Piyasa burada daha geniş anlamda, arz ve talebi birleştiği yer olarak ele alınmalıdır. Özgür ve açık kaynaklı yazılımı da içermektedir.

30. Bkz. Angwin, 2015, Yadron, 2014.

31. “Ankete katılanların %68’i uygulamalarının satışa sunulmasından itibaren 1000 dolardan az kazandığını ve katılımcıların %29’u uygulamalarının henüz hiç gelir getirmediğini ifade etmiştir” (App Promo, 2013). “Çoğu uygulama geliştiricileri ayda 500 dolardan daha az kazanmaktadır” (Molla, 2012). Ayrıca bkz. App Promo, 2012.

32. Karşılaştırınız : VI: [Konsey] “İlkelerin tamamlayıcı olduğunu ve bir bütün olarak alınması gerektiğini kabul etmektedir…”.

33. Örneğin virüs bulaşmış bir bilgisayar ya da cihaz başkalarının varlıklarına saldırı için kullanılabilir (dağılmış hizmet engelleme saldırıları) ve gizlilik saldırısı yoluyla kişisel verilerin ifşası verileri çalınan bireyleri ve vakaya maruz kalan kurumun ekonomik çıkarlarını etkileyebilir.

34. Girişimlerin uluslararası olarak karşılaştırmalı bir analizi için bkz. ACMA, 2011.

35. OECD, 2012d.

36. Tavsiye Metninin girizgahındaki “Düşünceli” ifadesi (10. paragraf) paydaşların dijital ortamın korunması adına sorumluluk paylaştıklarını vurgulamaktadır. “Toplu sorumluluk” kavramı ile ilgili daha fazla detay için bkz. ISOC, 2015.

37. United Nations, 1948, 1966a ve 1966b.

38. Tavsiye Metninin “güvenlik önlemleri” terimini dijital güvenlik risk yönetimi için alınan güvenlik önlemlerini ifade etmek için kullandığının altını çizmek gerekmektedir. Diğer türdeki güvenlik önlemleri metnin kapsamı dışındadır.

39. 2001 İnternet Politikası Oluşturma İlkeleri için Konsey Kararını (OECD 2011) açıklayan Bildiri şunu ifade etmektedir: “[...] İnternetin açık ve erişilebilir yapısının ifade özgürlüğünün yararına ve araştırma ve ekonomilerimize çok geniş alanda inovasyon sağladıkları için geliştirme de dahil olmak üzere bilginin, birikimin ve görüşlerin kullanıcılar tarafından paylaşılmasının sağlanması açısından desteklenmesi gerekmektedir [...]”. 2011 Tavsiye Metni ise “İnternet Ekonomisi için politikalarını geliştirirken ya da gözden geçirirken, Üyelerin diğer paydaşlarla işbirliği halinde şu yüksek düzel ilkeleri dikkate almaları tavsiye edilmektedir [:] [...] Şeffaflığı, adil yargılamayı ve hesap verilebilirliği sağlamak.” ifadesini kullanmaktadır. Bu noktada Bildiri ayrıca şunu ifade etmektedir: “İnternet ortamında kamu güvenini tesis etmek adına politika oluşturma süreçleri ve şeffaflık, adil yargılama ve hesap verilebilirlik sağlayan sağlam politikalar teşvik edilmelidir. Şeffaflık İnternet kullanıcılarının kendi hak ve çıkarları doğrultusunda zamanlı, erişilebilir ve hukuk dahilindeki bilgiye sahip olabilmelerini sağlamaktadır. Adil yargılama hakların tanımı, beyanı ve savunulmasının idaresinde öngörülebilir karar alma süreçleri sağlamaktadır. Hesap verilebilirlik ise tarafları uygun olan durumlarda İnternet üstündeki eylemler için hesap verebilir hale getiren politikalar vasıtasıyla sağlanmaktadır.”

40. OECD 2013b, Bölüm Üç, paragraf 15 a).

41. İşbirliği 2002 Güvenlik Ana Esaslarında kullanışlı bir kavram olarak vurgulanmıştır. Bu Tavsiye Metninde ise artan öneminin ve diğer İlkeleri desteklemedeki önemli rolünün altını çizmek amacıyla İlke haline getirilmiştir.

42. İlginç bir örnek olarak, bir Kore BAME konsorsiyumu olan, 1996 yılında güvenlik ile ilgili ortak çıkarlar hususunda ortakları ile bilgi paylaşımı ve işbirliğinde bulunmak üzere kurulmuş olan CONCERT verilebilir. CONCERT Kore'deki 300'ün üstünde bilgi güvenlik ünitesini, ilgili enstitüleri ve yönetimleri barındırmaktadır. Bkz.www.concert.or.kr.

43. Birleşik Krallık Siber Güvenlik Bilgi Paylaşım Ortaklığı (CiSP) gibi. Bkz.www.cert.gov.uk/cisp.

44. "Kamu-özel" ifadesindeki "özel" terimi işletmeler, kar amacı gütmeyen kurumlar, sivil toplum, akademi, teknoloji camiası vs. gibi paydaşları içermektedir.

45. Risk "müdahalesi" bazen risk "azaltımı" gibi farklı ifadelere sahip olabilmektedir. Terminoloji ve tanımlar için bkz. Kutu 3. Risk müdahalesi ile ilgili diğer terimler şunları da kapsamaktadır: riski kabul etmek, almak ya da üstlenmek; riski azaltmak, küçültmek ya da minimize etmek; riski transfer etmek ya da yeniden tahsis etmek; riski engellemek ya da yok etmek.

46. OECD/Eurostat, 2005.

47. Piper, 2014.

EKONOMİK İŞBİRLİĞİ VE KALKINMA ÖRGÜTÜ (OECD)

OECD, küreselliğin getirdiği ekonomik, sosyal ve çevresel güçlüklere hitap edebilmek adına birlikte çalışabildiği özel bir forumdur. OECD aynı zamanda şirket yönetimi, bilgi ekonomisi ve yaşlanmakta olan nüfusun getirdiği güçlükler gibi yeni gelişmelere ve endişeleri anlamak ve devletlerin bunlara cevap verebilmesine yardımcı olmak adına yapılan girişimlerin de öncüsü konumundadır. Örgüt hükümetlerin politika deneyimlerini karşılaştırabilecekleri, ortak sorunlara çözüm arayabilecekleri, iyi uygulamaları tanımlayabilecekleri ve yerel ve uluslararası politik işbirliği için çalışabilecekleri bir ortam sunmaktadır.

OECD üye ülkeleri şunlardır: Avustralya, Avusturya, Belçika, Kanada, Şili, Çek Cumhuriyeti, Danimarka, Estonya, Finlandiya, Fransa, Almanya, Yunanistan, Macaristan, İzlanda, İrlanda, İsrail, İtalya,
Japonya, Kore, Lüksemburg, Meksika, Hollanda, Yeni Zelanda, Norveç, Polonya, Portekiz, Slovak Cumhuriyeti, Slovenya, İspanya, İsveç, İsviçre, Türkiye, Birleşik Krallık ve Amerika Birleşik Devletleri. Avrupa Birliği de OECD çalışmalarında yer almaktadır.

OECD Yayınları geniş bir şekilde Örgütün istatistik toplama ve ekonomik, sosyal ve çevre alanındaki araştırmalarının yanında üyelerinin üzerinde uzlaştığı sözleşmeler, rehberler ve standartları yaymaktadır.

Bu OECD Tavsiye Metni ve Yardımcı El Kitabı tüm paydaşlar için dijital güvenlik riskinin ekonomik ve sosyal refah boyutunda rehberlik sağlamaktadır. Dijital ekonominin büyüme, refah ve kapsayıcılık için oldukça önemli bir hale geldiği bu ekonomik bağlamda, dijital güvenlik riski daha geniş bir ekonomik ve sosyal perspektifte ve bu riskin yönetimi de paydaşların karar alma süreçlerinin parçası olarak ele alınmalıdır.

Bu kitabın orijinal versiyonu aşağıdaki başlıklarla yayınlanmıştır:
Digital Security Risk Management for Economic and Social Prosperity.OECD Recommendation and Companion Document/La gestion du risque de sécurité numérique pour la prospérité économique et sociale.Recommandation de l'OCDE et document d'accompagnement © 2015, Organisation for EconomicCo-operation and Development (OECD), Paris.

İngilizce versiyonu: ISBN 9789264245358/DOI: http://dx.doi.org/10.1787/9789264245471-en
Fransızca versiyonu: ISBN 9789264246096/DOI:http://dx.doi.org/10.1787/9789264246089-fr

Bu kitabın çevirisi OECD ile yapılan anlaşma üzerine yapılmıştır. Bu, resmi bir OECD çevirisi değildir.

www.oecdbookshop.org - OECD online kitabevi
www.oecd-ilibrary.org - OECD online-kütüphanesi
www.oecd.org/oecddirect- OECD başlık uyarı hizmeti

T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

OECD
BETTER POLICIES FOR BETTER LIVES