Yeni dönemde teknoloji ve siber risklere odaklanmak

EY nasıl destek olabilir?

Ağustos 2020

EY
Building a better working world

İçindekiler

Giriş

Merhaba,

Öncelikle tüm dünyada ve ülkemizde COVID-19 salgınının etkilerinin devam ettiği bir dönemde sağlıklı günler dileriz. Salgının insan yaşamı üzerine olan etkileri ilgili uluslararası organizasyonlar ile devletimiz kurum ve kuruluşları tarafından yakından takip edilmekte ve gerekli yönlendirmeler kamuoyuna yapılmaktadır.

Normalleşme adını verdiğimiz, salgının etkilerinin muhasebesinin yapıldığı ve kısa, orta ve uzun vadede hayatımızda geçici ya da kalıcı nasıl değişikliklere yol açacağının değerlendirildiği bu aşamada sürdürülebilirlik en öne çıkan kavram gibi görünmektedir.

İçinden geçtiğimiz dönem başta insan hayatı olmak üzere yaşama dair birçok kritik unsurun muhafaza edilmesi ve sürdürülebilirliğinin sağlanması, olumsuz etkilerinin en aza indirgenmesi açısından her zaman karşılaşılabilecek bir vaka değildir. Bununla birlikte risk yönetimi açısından ele alınması gereken bir durum olarak nitelendirilebilir. Bu vaka umarız kısa sürede ortadan kalktığında iş dünyası açısından yeni bir döneme girileceği üzerinde mutabık kalınmış bir olgu olarak ortaya çıkmaktadır. Bu yeni dönemin özellikleri aşağıdaki şekilde tezahür edebilir:

- İnsan sağlığı ve refahı ile iş dünyasındaki yavaşlama ve talep azalmasının etkilerinin aynı anda değerlendirilebileceği bir el kitabı bulunmamaktadır. Mevcut Kurumsal Risk Yönetimi yaklaşımları ve İş Sürekliliği planları bu durumu yönetmek için yeterli olmayabilir.
- Hedeflenecek kilometre taşları eskisi kadar keskin olmayabilir; projeler için uzun hazırlık, planlama, ihale ve yürütme süreçleri yerini daha hızlı çözümlere bırakacaktır.
- Her gün hem insanlık hem de iş dünyası için yeni bir başlangıç olarak tanımlanabilir. Paydaşlar, Yönetim Kurulu, düzenleyiciler, çalışanlar ve kamuoyu için yönlendirmeler günlük ve hareket halindeyken oluşturulur.
- Yeni risk alanları daha hızlı ortaya çıkıp çok çevik şekilde aksiyon almayı gerektirir. Yasal düzenlemelere uyum hiç olmadığı kadar önemlidir.
- Uzaktan çalışma ve mobil işgücünün nihayet kelime anlamını bulması sonucu buna göre şekillenecek iş yapış şekillerinde teknoloji ve siber dünyaya ait riskler öncelikli konular arasındadır.

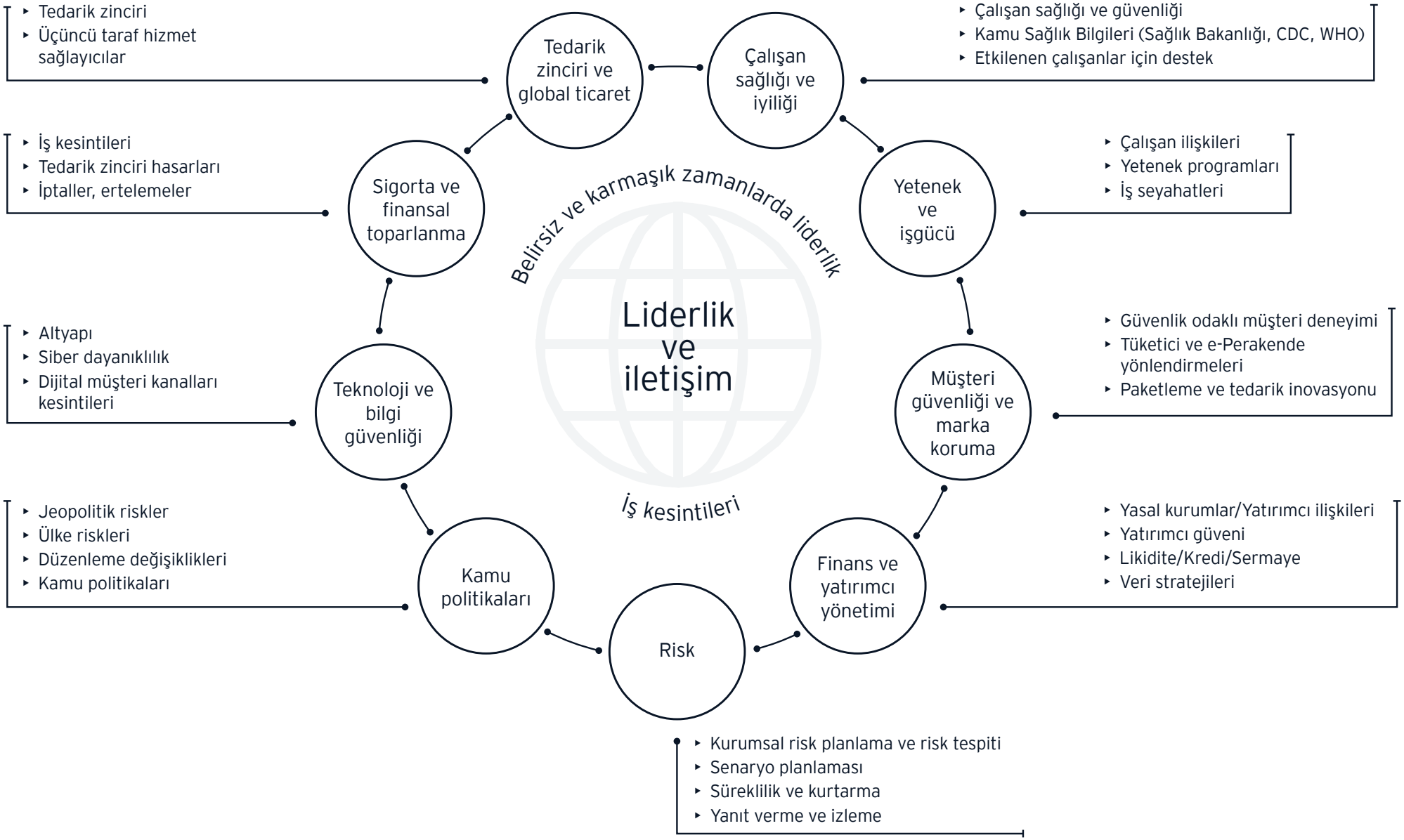
Bu çerçevede EY olarak karşımıza çıkacak ve kalıcı değişiklikler getirecek bu yeni döneme hazırlık anlamında yaklaşım üretme çabalarımızdan biri olarak "Yeni dönemde teknoloji ve siber risklere odaklanmak" başlıklı bu paketi dikkatinize sunmaktan memnuniyet duyarız.

Ümit Yalçın Şen
EY Türkiye
Şirket Ortağı
Siber Güvenlik Hizmetleri Lideri

Yeni dönemde teknoloji ve siber güvenlik kaynaklı riskler

EY bakış açısı

EY kurumsal dayanıklılık çerçevesi



Teknoloji riskleri

Devamlılığı artırmak, bulut kullanımı ve ağı yeniden keşfetmek

- Bir kriz sırasında bile müşterilerin teknoloji ürün ve hizmetlerine erişim beklentileri hızla artmaktadır.
- Kullanıcı merkezli, mobil, çevik ve veri odaklı özellikler her kuruluş için minimum gereksinimlerdir.
- Kesintiler meydana geldiğinde teknoloji, şirketinizin sürekliliği, iyileşmesi ve hayatta kalması için önemli bir olanak sağlar.

1

Teknoloji nasıl etkilenebilir?

- Aşırı iş gücü hareketliliği ve uzaktan kullanıcı erişimi, olağandışı ve ön görülemeyen ağ trafiği veya hizmetlerin aksaması
- Üçüncü taraf iş ortakları ve hizmet sağlayıcılar olarak çeşitli teknoloji ürünlerinin, hizmetlerinin ve lisanslarının yetersizliği, çalışmaya devam edememesi veya talebi karşılayamaması
- Yardım masası, son kullanıcı talepleri ve ekipman/donanım destek ihtiyaçlarının artması ve diğer ihtiyaçlar nedeniyle teknolojik operasyon desteğinde kesinti

2

Teknoloji devamlılığı çözüm alternatifleri

- **Talep bazlı ölçeklenebilirlik**
  Altyapı, ağ ve işlem gücünde talep edilen ani artışlara hitap edecektir.
- **İş odaklı çeviklik**
  Yazılım-tanımlı (software-defined) ya da katmanlı mimari teknolojilerinden yararlanmak, altyapının yeniden şekillendirilmesine olanak tanınmasına imkan verebilir.
- **Süreç otomasyonu**
  Altyapı ve genel BT operasyonlarına manuel müdahaleyi en aza indirerek, azalan BT iş gücünü yönetebilmek için alternatiflere sahip olunabilir.

3

Dikkat edilmesi gerekenler

- Altyapı hizmetlerinin (ör: ağ, sistemler) yetenek ve iş yükü değerlendirilmesi
- Talep artışını ve çevikliği desteklemek için altyapı güncellemeleri
- Kritik teknoloji bağımlılığı analizi
- Yazılım tanımlı ve katmanlı otomasyon teknolojisi etkinleştirmesi
- Açık konular için tamamlayıcı teknoloji kaynağı ve üçüncü taraf tedarikçi temini
- Üçüncü taraf teknoloji tedarikçileri için devamlılık/süreklilik değerlendirmeleri

Siber devamlılık: Salgın kaynaklı endişeler

Salgın süresince karşılaşılabilecek siber riskler

Salgınlar benzersiz olaylardır; bir kuruluşun güvenli operasyonları, iletişimi, üretkenliği ve devamlılığı sürdürme yeteneği bu dönemde kritiktir.

Çalışma sahaları/uzak çalışma ortamları

İş gücünü şirket içi bir modelden uzak bir modele kaydırmak yeni tehditler ve zorluklar getirir. Bir altyapının artan trafik yükünü kaldıramaması önemli bir husustur. Ayrıca, yeterince güvenli olmayan ev bilgisayarları, kurumsal ağda risklere neden olabilecektir.

3. Parti sürekliliği

Üçüncü taraf hizmetleri engellenebilir, sınırlandırılabilir veya devre dışı bırakılabilir. Bu nedenle, coğrafi olarak dağınık bölgelerde hizmet sağlayıcıların olması gerekebilir. Kritik hizmetler için, birden fazla / yedekli tedarikçi tercih edilebilecektir.

Genişletilmiş/gelişmiş kimlik ve erişim yönetimi (IAM)

Yetkilendirme, kimlik doğrulama ve erişim denetimleri, işgücünü alternatif lokasyonlarda barındıracak şekilde tesis dışındaki yerlere güvenli bir şekilde genişletilebilir.

Veriler düzenli olarak ve güvenli bir şekilde tesis dışında yedeklenmeli ve birincil sisteme, zamanında, doğru ve güvenli bir şekilde geri yüklenebilmelidir.

Acil durum döneminde iletişim erişimini ve politika uyumunu sürdürmek için ağlar, erişim ve yetkilendirme sistemleri, uygulamalar, veri kaybını önleme sistemleri, güvenlik duvarları ve saldırı tespit ve önleme sistemleri gibi altyapı sağlam ve yedekli olmalıdır.

Bir ihlal veya tehdit tespit edildiğinde, uygun kontroller tehditin kısıtlanmasını, bertaraf edilmesini ve kurumun harekete geçmesini sağlamalıdır.

Zafiyetli veya sınırlı altyapı

Siber tehdit aktörleri, savunmasız olarak algılanan ve beklenmedik koşullar altında kendilerini savunamayan hedeflerden yararlanmaya çalışır. Bu, çalınan fikri mülkiyet, hassas verilerin ele geçirilmesi veya kritik altyapının sabote edilmesi ile sonuçlanabilir.

Sürekli veri ihlali riski

Depolanan veya taşıma sürecinde verileri uygun şekilde korumayan ya da hiç önlem almayan kurumların dışarıda çalışan işgücü nedeniyle veri ihlali ya da kaybına maruz kalma olasılığı artar. Personel ve kaynak azaltımı nedeniyle bu tür olayların büyüklüğü ve etkisi artabilir.

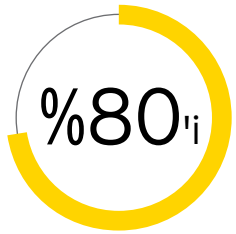
Uyarlanabilir SOC ve olay yanıtı

Bir salgın sırasında güvenlik operasyon merkezi (SOC) kaynakları sınırlı olacaktır. Sonuç olarak kurumlar, alışılmadık ortamlarda, altyapılarda, insanlarda ve süreçlerde karşılaşılan yeni sorunlara yanıt vermek için farklı SOC yapılarına (farklı bölgelerde) güvenmek zorunda kalabilir.

Yönetim; politikaların, kaynakların, altyapının ve kontrollerin yeterince korunduğunu ve baskı sırasında sürdülebilir olduğundan emin olmalıdır.

Kuruluşlar, çalışanlardan, üçüncü taraflardan, tehdit aktörlerinden ve diğer anormalliklerden gelen olayları algılama ve izleme yeteneğine sahip olmalıdır.

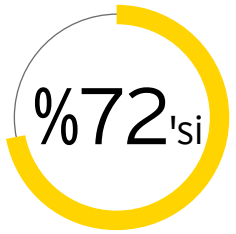
Dünyadaki kurumların



salgın tipi bir olay olması durumunda iş sürekliliği için hazırlıksızdır.

Kaynak: Basex

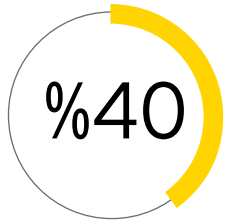
Çok uluslu şirketlerin



henüz bir salgın krizine hazırlanmadı.

Kaynak: Continuity Central

Bir salgın, olası personel devamsızlığını uzun dönemde



artırabilir.

Kaynak: Gartner

Bir salgın tek seferlik bir olay değildir ve hastalık dönemleri **3** ila **12** ay arayla **2** veya **3** dalga halinde gelebilir.

Bir salgının toplam süresinin **12** ila **18** ay olması muhtemeldir.

Kaynak: Canadian Centre for Occupational Health and Safety

Siber devamlılık: Salgın kaynaklı endişeler

Tehdit ve risklere karşı olası risk azaltıcı faaliyetler

Uzaktan çalışmayı mümkün kılan cihazların güncel **yama ve güvenlik konfigürasyonlarına** sahip olunması

VPN bağlantılarında 2+ Faktörlü Kimlik Doğrulama kullanımı, mümkün değilse uzaktan çalışan personelin **güçlü parolalar** kullandığından emin olunması

VPN kapasitesinin BT güvenlik ekiplerince test edildiğinden emin olunması

Yüksek yetkili erişimlerin düzenli olarak izlenmesi

Security Information and Event Management (SIEM) sistemleri kullanımı, **Güvenlik Operasyon Merkezi (Security Operation Center SOC)** ekibi için personel ihtiyacının değerlendirilmesi

Log gözden geçirme, saldırı tespit, olay müdahale ve kurtarma gibi siber güvenlik faaliyetlerine daha fazla önem gösterilmesi

Çalışanların **oltalama saldırıyla** ilgili uyarılması, özellikle **Coronavirüs ile ilgili web siteleri ve e-postalar** gibi zararlı yazılım ihtiva etmesi muhtemelen ortamlara karşı uyarılar yapılması

Web ve e-posta güvenliği için filtreleme teknolojileri kullanılması

Yönetici (admin) erişim ve faaliyetlerini zorlaştırılması, gerçek ihtiyaca göre kuralların yeniden gözden geçirilmesi

Acil durum ve kriz yönetimi yetkinliklerininin güncellenmesi, **sistem ve veri yedeklerininin** kontrol edilmesi

Son kullanıcı güvenliğine önem gösterilmesi

En kötü senaryoları düşünün, kriz yönetimi ve olay müdahale planlarınızı ve kritik tedarikçilerinizin erişilebilirlik durumlarını buna göre yeniden değerlendirin.

Yeni dönemde uzaktan çalışmak

Veri gizliliğini korumak (1/2)

COVID-19 (Coronavirus) virüsünün yayılmasına bağlı olarak tüm dünyada kamu otoriteleri sosyal mesafenin korunması ve toplu halde bulunulan yerlerde faaliyetlerin (işyerleri, sinema ve tiyatrolar, kafeler gibi) durdurulması gibi bir dizi önlem almış durumdadır.

Bu durum, çeşitli sektörlerde faaliyet gösteren EY dahil pek çok kurumun çalışanlarını uzaktan çalışma sistemine geçirmek zorunda kalmasına neden olmuştur.

Uzaktan çalışırken kullanılan verilerin gizliliklerinin korunması elzemdir. Veri koruma ve mahremiyet hususlarında iyi uygulamalara ek olarak, müşterilerinizin ve firmanızın verilerini güvence altına alabilmeniz için birtakım ek önlemler gündeme gelmelidir.

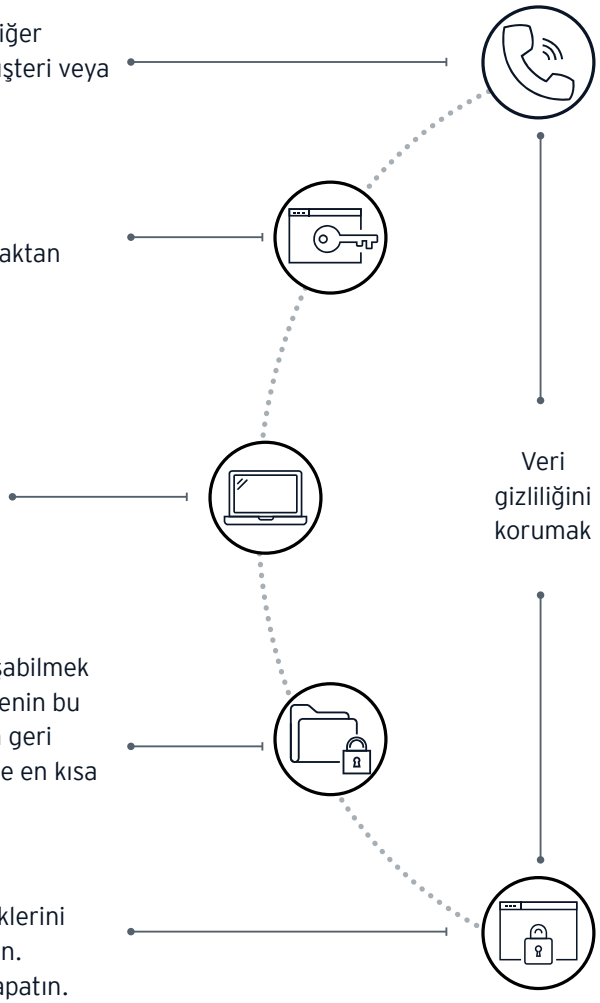
Gizli bilgilerin konuşulacağı görüşmelerde dikkatli olun. Diğer insanlardan ya da hane halkından uzaklaşamıyorsanız müşteri veya tedarikçi adı vermekten kaçının.

Ekranınızın başka insanlarca görülmediğinden emin olun. Pencerelerden ekranınızın görülebileceği odalarda çalışmaktan kaçının.

Video konferans yaptığınız durumlarda karşı tarafın herhangi bir gizli bilgi görmediğinden emin olun.

Gizli dökümanların basılı kopyalarından kaçının! Eğer çalışabilmek için basılı kopyaya ihtiyacınız varsa, etrafınızdaki hiç kimsenin bu kopyaları göremeyeceğinden emin olun. Kopyaları hemen geri dönecek olsanız dahi mutlaka güvenli bir yerde saklayın ve en kısa zamanda ofise geri götürün.

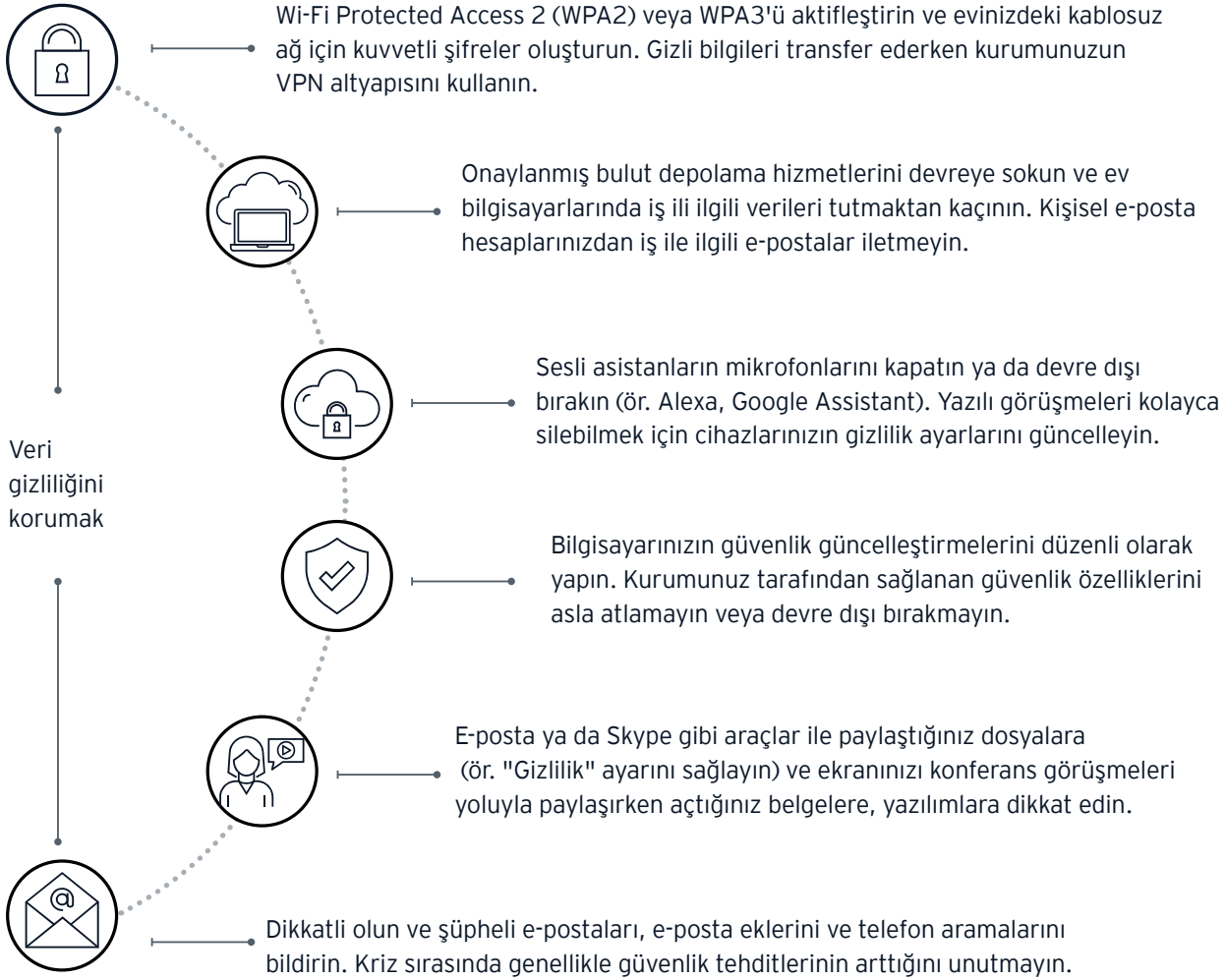
Bilgisayarınızı güvenli bir ortamda saklayın ve hırsızlık risklerini en aza indirmek için bir güvenlik kilidi almayı değerlendirin. Gözetimsiz bırakacağınız zaman bilgisayarınızı mutlaka kapatın.



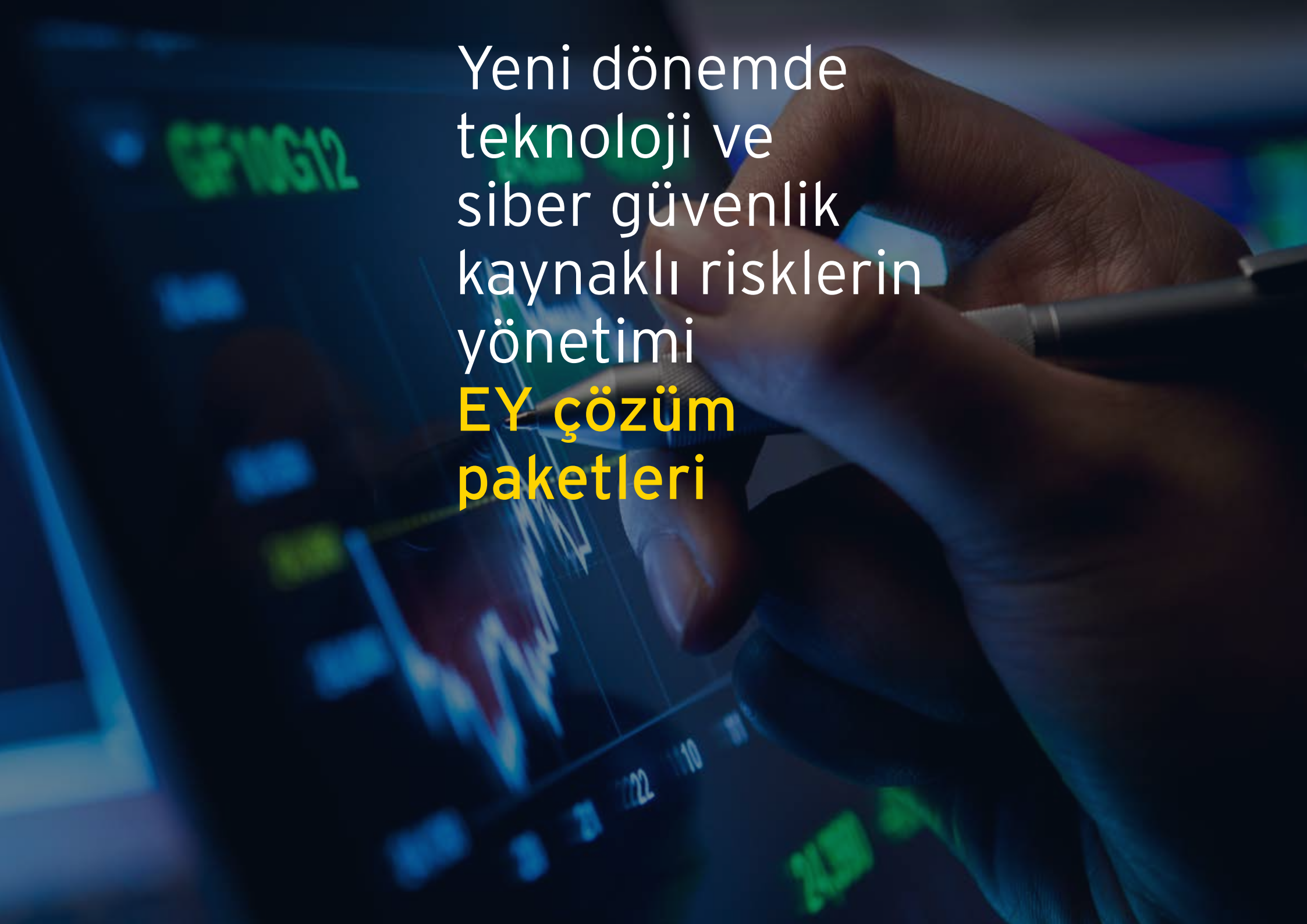
Yeni dönemde uzaktan çalışmak

Veri gizliliğini korumak (2/2)

Kullandığınız Teknolojileri güvenliği gözetecek şekilde ayarlayın ve güvenlik iyi uygulamalarını benimseyin. Teknoloji uzaktan çalışmanızı sağlayan anahtar unsurlardan biri. Aşağıdaki iyi uygulamalar ile verilerinizi güvenli bir şekilde taşıyabilir ve aktarabilirsiniz:



- İşveren olarak, uzaktan çalışma için veri koruma ve mahremiyet konularında rehberlik edin.
- Çalışan olarak günceli takip edin ve verilen önerileri takip edin.
- Veri koruma ve mahremiyete dair önlemlerinizi müşteri ve tedarikçileriniz ile paylaşın. Müşterilerinizden gelecek yönergeleri gerektiği gibi uygulayın. Veri ihlali gibi güvenlik olaylarını derhal uygun şekilde kurumunuzun bilgi güvenliği birimlerine iletin.



Yeni dönemde teknoloji ve siber güvenlik kaynaklı risklerin yönetimi

EY çözüm paketleri

Teknoloji ve siber dayanıklılık çerçevesi

Şimdi, sonrası ve uzun vade için öneriler

- Uzaktan çalışma ortamlarının güvenli hale getirilmesine destek
- Teknoloji altyapısı sürekliliği tasarımı
- Teknoloji ve siber krizlere hazırlanmak açısından simülasyonları
- COVID-19 temalı zararlı yazılım analizi
- Bulut geçişi teknoloji ve siber risk analizi
- Mahremiyet Etki Analizi (yeni çalışma yöntemleri için)
- Siber Güvenlik ve Privacy farkındalık eğitimleri

- Sızma testi ve zafiyet analizleri (başta uzaktan çalışma ortamları ve bulut ortamları için)
- Hızlı teknoloji süreklilik analizi
- Üçüncü taraf risk analizleri ve izleme desteği

- Teknoloji ve siber güvenlik log inceleme ve aksiyon belirleme desteği

- Siber güvenlik olay müdahale desteği
- Siber kriz yönetimi desteği
- Siber forensic (adli bilişim) desteği

- Teknoloji ve iş etki analizleri ve süreklilik planları güncellemesine destek
- Şimdi ve yakın gelecek için siber güvenlik politikaları güncellemeleri
- Teknoloji mimarisi iyileştirmeleri (performans ve güvenlik odaklı)

Teknoloji ve siber dayanıklılık çerçevesi

Şimdi, sonrası ve uzun vade için öneriler – Teknoloji

Şimdi (1-3 ay)

Mekan, cihaz ve iş gereksinimi bağımsız çalışma

- İş faaliyetlerinin desteklenmesi için yeterli bant genişliği ve sürekliliği için BT altyapı tasarımı ve konfigürasyonu
- Uzak çalışma teknoloji optimizasyonu
- Masaüstü ve erişim (ör: VPN, RDP, vb.) yetkinliklerinin yaygınlaştırılması
- BT altyapı kaynaklarının iş kritikliğine ve ihtiyaçlarına göre adaptasyonu

Sonra (3-6 ay)

Talep bazlı, yüksek erişimli ve hızlı altyapı çözümleri planlaması

- Bulut ve altyapı teknolojileri modernizasyonunun hızlandırılması
- Yazılım tanımlı ağ mimarisine geçişin planlanması
- Daha akıllı ve daha çevik çalışmak adına kurumsal işbirliği platformlarının gözden geçirilmesi

Uzun vade (6+ ay)

BT operasyonları için otomasyon ve yapay zeka desteği

- BT altyapısında mimari değişiklikler (bulut, sanallaştırma, vb) ve BT operasyonlarının self-servise geçmesi ya da otomasyonu (uygulama yükleme, servis etkinleştirme, vb.)
- Otomasyon verimliliği için orkestrasyon
- BT altyapısı ve uygulamaların davranışları için yapay zeka ve makine öğrenme ile gerçek zamanlı izleme ve müdahale

Teknoloji ve siber dayanıklılık çerçevesi

Şimdi, sonrası ve uzun vade için öneriler – Siber güvenlik

Şimdi (1-3 ay)

Uzaktan çalışmayı desteklemek

- Politika ve prosedürler
- Siber farkındalık kampanyaları
- Uzaktan çalışmak için kullanılan bilgisayar ve cihazlar için özel güvenlik standartları
- Güvenli son kullanıcı güvenliği
- Güncellenmiş izleme yetkinlikleri
- Daha sık ve yakından takip edilen zafiyet yönetimi
- Güvenli uzaktan çalışma platformları
- Üçüncü taraf desteği

Sonra (3-6 ay)

Gelecek için planlama ve geçiş dönemi aksiyonlar

- Güncellenmiş risk haritası
- Siber güvenlik stratejisi ve yol haritası
- Güncellenmiş uzak çalışma platformları
- Cloud geçişleri için analizler
- Güncellenmiş yama ve versiyon geçiş stratejileri
- Kaynak planlama ve anlaşmaların gözden geçirilmesi

Uzun vade (6+ ay)

Yeni dönem için revize edilmiş siber güvenlik fonksiyonları

- İş birimlerine danışmanlık ve öncülük yapan siber güvenlik yaklaşımı
- Güvenlik yönetişim ve operasyon yapısında güncellemeler
- Risk değerlendirme yaklaşımında güncellemeler
- Siber güvenlik performans değerlendirmeleri için yeni KPI'lar

Teknoloji ve siber dayanıklılık yaklaşımı

Şimdi, sonrası ve uzun vade için hizmetlerimiz

Uzaktan çalışma sürdürülebilirlik destek çalışmaları

- Uzaktan çalışma ortamlarının güvenli hale getirilmesine destek
- Hızlı teknoloji süreklilik analizi
- Teknoloji ve siber krizlere hazırlık simülasyonları

3. Taraf risk analizleri ve sürdürebilirlik desteği

- Üçüncü taraf risk analizleri
- Üçüncü teknik yeterlilik analizleri
- Üçüncü taraf sözleşme yönetimi desteği
- Üçüncü taraf izleme ve değerlendirme desteği

Geçiş dönemi çalışmaları

- Mahremiyet Etki Analizi (yeni çalışma yöntemleri için)
- Bulut geçişi teknoloji ve siber risk analizi
- Geçiş dönemi için siber güvenlik politikaları güncellemeleri

Orta – Uzun vade hazırlık çalışmaları

- Teknoloji ve iş etki analizleri ve süreklilik planları güncelleme
- Teknoloji mimarisi iyileştirmeleri (performans ve güvenlik odaklı)
- Siber güvenlik mimari dönüşüm çalışmaları

Siber güvenlik risk analizleri

- COVID-19 temalı zararlı yazılım analizi
- Sızma testi, zafiyet analizleri ve siber risk incelemeleri (başta uzaktan çalışma ortamları ve bulut ortamları için)
- Siber güvenlik olay müdahale ve kriz yönetimi desteği

Siber güvenlik mühendislik desteği

- Teknoloji ve siber güvenlik log inceleme ve aksiyon belirleme desteği
- Siber güvenlik mimari tasarımı ve değerlendirme
- Siber güvenlik çözümleri uyarlama desteği, konfigürasyon analizi
- Siber forensic (adli bilişim) desteği

Teknoloji risk ve uyum destek çalışmaları (BDDK, GİB, SPK, KVKK mevzuatları uyarınca)

Siber güvenlik ve Kişisel Veri Koruma farkındalık eğitimleri

Hemen (0 -3 ay) | **Geçiş dönemi** (3-6 ay) | **Orta-Uzun vade** (6+ ay)

Teknoloji ve siber dayanıklılık yaklaşımı

Hemen (0-3 ay) gündeme alınabilecek konular (1/3)

Hizmet adı	Uzak çalışma ortamları güvenliği
Sektör odağı	Tüm sektörler
Muhtemel süre	**1-2** hafta
Hizmet içeriği	▸ Kurum için uzak çalışma (iletişim, haberleşme, doküman yönetimi, vb.) çözümlere ilişkin mimari, altyapı, uygulama ve veri güvenliği standartlarının belirlenmesi ▸ Mevcut çözümlerinin kapasite ve erişilebilirlik analizleri, tasarımına destek verilmesi ▸ Uzak çalışma prosedürlerinin oluşturulması ▸ Uzak çalışma güvenliği bilgilendirme ve farkındalık eğitimleri

Hizmet adı	Teknoloji sürekliliği analizi ve desteği
Sektör odağı	Tüm sektörler
Muhtemel süre	**2-4** hafta
Hizmet içeriği	Teknoloji sürekliliği ve dayanıklılığı hazırlıkları açısından kurumunuzun mevcut durumunu anlamak için aşağıda belirtilen konular kapsamında değerlendirmeler ve analizler gerçekleştirilecektir: ▸ İş ve BT faaliyetleri ▸ Yönetişim ve kaynak planı ▸ Siber Güvenlik ▸ BT kapasitesi ve uzak çalışma ▸ İletişim ve haberleşme ▸ DDOS ve yük testleri

Teknoloji ve siber dayanıklılık yaklaşımı

Hemen (0-3 ay) gündeme alınabilecek konular (2/3)

Hizmet adı	Siber güvenlik risk analizleri
Sektör odağı	Tüm sektörler
Muhtemel süre	**1-4** hafta (kapsama göre değerlendirilmelidir)
Hizmet içeriği	**COVID-19 temalı zararlı yazılım analizi** ▸ Güncel siber güvenlik tehdit bültenleri ve istihbarat kanalları taranarak COVID-19 iletişimi üzerinden gelebilecek zararlılara karşı analizlerin gerçekleştirilmesi **Sızma testi & zafiyet analizleri** ▸ Uzak çalışma altyapısı ▸ Bulut sistemleri ▸ Son kullanıcı ekipman ve cihazları ▸ Mobil ve web uygulamalar (ör: OWASP Top 10) **Siber güvenlik olgunluk analizi** ▸ EY, NIST vb. çerçevelere göre hızlı analizler (benchmarklar)

Hizmet adı	Teknoloji ve siber kriz hazırlığı/desteği
Sektör odağı	Tüm sektörler
Muhtemel süre	**1-2** hafta
Hizmet içeriği	▸ Gerekli olan durumlarda kriz yönetim desteği ▸ Teknoloji ve siber kriz senaryolarının hazırlanması ▸ Teknoloji ve siber kriz simülasyonları ▸ Teknoloji ve siber kriz yönetimi desteği ▸ İç ve dış paydaşlara yönelik kriz iletişim desteği

Teknoloji ve siber dayanıklılık yaklaşımı

Hemen (0-3 ay) gündeme alınabilecek konular (3/3)

Hizmet adı	3. taraf risk ve izleme desteği
Sektör odağı	Tüm sektörler
Muhtemel süre	**2-4** hafta
Hizmet içeriği	▸ Kuruma hizmet verilen BT hizmet sağlayıcılarının envanteri hazırlığı ▸ Hizmet tiplerine göre gruplandırma, risk analizi ve teknik yeterlilik değerlendirme kriterlerinin belirlenmesi ▸ Örneklem bazlı risk analizleri ve teknik yeterlilik analizleri ▸ Kritik olanlar için bağımlılık ve alternatif tedarikçi analizleri ▸ Hizmet sağlayıcı performans izleme kriterleri belirleme, kontrol ve denetim süreçleri hazırlığı

Hizmet adı	Siber güvenlik mühendislik desteği
Sektör odağı	Tüm sektörler
Muhtemel süre	**2-4** hafta
Hizmet içeriği	▸ Siber güvenlik mimari tasarım değerlendirme ve iyileştirme desteği ▸ Teknoloji altyapısı ve siber güvenlik log inceleme ve aksiyon belirleme desteği ▸ Yüksek yetkili erişim kontrol ve loglama kural seti belirleme ve izleme desteği ▸ Siber güvenlik çözümleri uyarlama desteği, konfigürasyon analizi (ör: DLP kurulum ve konfigürasyon) ▸ Siber forensic (adli bilişim) inceleme desteği

Teknoloji ve siber dayanıklılık yaklaşımı

Geçiş dönemi (3-6 aylar arası) çalışmaları

Hizmet adı	**Siber güvenlik dönüşüm desteği**
Sektör odağı	Tüm sektörler
Muhtemel süre	**~6** hafta
Hizmet içeriği	▸ Bulut geçişi için tedarikçi ve veri merkez güvenlik analizleri ▸ Bulut ortamına geçebilecek uygulama ve sistemler için geçiş sonrası siber risk değerlendirmeleri ▸ Yeni çalışma modelleri ve (bulut dahil) güncellenen BT ortamları ve süreçler için Mahremiyet Etki Analizleri (KVKK ve GDPR uyarınca) ▸ Yeni döneme geçiş için siber güvenlik politika ve prosedür geliştirme desteği ▸ Yeni dönemde geçerli olabilecek Siber Güvenlik risk ve kontrollerinin belirlenmesi

Teknoloji ve siber dayanıklılık yaklaşımı

Orta-Uzun vade (6 ay ve sonrası) hazırlık çalışmaları

Hizmet adı	Teknoloji ve iş sürekliliği dönüşümü
Sektör odağı	Tüm sektörler
Muhtemel süre	**6-8** hafta
Hizmet içeriği	Salgın sonrası dönem için teknoloji sürekliliğinde iyileşme amacıyla: ▸ Teknoloji bağımlılık analizi ▸ İş süreçleri/faaliyetleri ve teknoloji eşleştirmesi ▸ Teknoloji süreklilik planlarının hazırlanması ▸ Teknoloji sürekliliği iyileştirmeleri için kapasite ve performans analizleri, ek kapasite için maliyet analizleri ▸ Teknoloji yedekliliği stratejileri (yedek veri merkezi, yedekleme planları, vb.) ▸ Teknoloji sürekliliği test senaryoları ve planları

Hizmet adı	Teknoloji ve siber güvenlik mimari dönüşümü
Sektör odağı	Tüm sektörler
Muhtemel süre	**6-8** hafta
Hizmet içeriği	Teknoloji ve siber güvenlik mimarisi iyileştirmeleri ▸ Yazılım tanımlı mimari geçişleri ▸ Bulut dönüşümleri analizleri ▸ Uygulama, orta katman ve altyapı mimari değerlendirme ▸ Ağ mimarisi ve ayrıştırma stratejisi ▸ Siber güvenlik mimarisi analizi (katmanlı, BT/OT ayrımı, veri iletişimi ve gizliliği)

Teknoloji ve siber dayanıklılık yaklaşımı

Teknoloji ve siber risk uyum destek çalışmaları

Hizmet adı	Teknoloji risk ve uyum destek çalışmaları
Sektör odağı	▸ Bankalar ▸ Ödeme ve e-Para Şirketleri ▸ Finansal Kurumlar (Faktoring, Leasing, Finansman) ▸ E-Belge Özel Entegratörleri ▸ Portföy Yönetimi ve Yatırım Şirketleri ▸ Halka Açık Şirketler
Düzenlemeler	▸ TCMB - Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ ▸ BDDK – Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik ▸ BDDK – Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ ▸ GİB e-Belge Özel Entegratörleri Bilgi Sistemleri Denetimi Kılavuzu ▸ SPK Bilgi Sistemleri Yönetimi ve Denetimi Tebliğleri

Fark analizi

- Mevcut durumun değerlendirilmesi ve eksikliklerin tespiti
- Düzeltici aksiyon planlarının ve iyileştirme yol haritasının oluşturulması

Uygulama ve teknoloji desteği

- Uyum programının hayata geçirilmesine destek verilmesi
- Organizasyon, süreç ve sistemlere yönelik yönetişim çerçevesi, politika, prosedür ve envanterlerin hazırlanması
- İlgili personel eğitimlerinin verilmesi (ör: Bilgi güvenliği)
- Yol haritası ve uyum programının teknolojiyle/araçlarla desteklenmesi (GRC, Kimlik ve Erişim Yönetimi, Talep Yönetimi, Değişiklik Yönetimi, Log Yönetimi, Güvenlik Sistemleri vs.)
- Seçilen teknolojinin/araçların kurulumu ve uyarlanması

Sızma testi

- Sızma ve güvenlik testlerinin düzenlemelere uygun olarak gerçekleştirilmesi
- Tespit edilen açıklıkların giderilmesine destek verilmesi

Ön denetim/Denetim

- İhtiyaçlar doğrultusunda ön denetim faaliyeti gerçekleştirilmesi ve bulguların raporlanması
- Mevzuata uygun olarak bağımsız denetim ve raporlama faaliyetlerinin gerçekleştirilmesi
- Hizmet firmaları için ISAE3402, SSAE18 (SOC2 ve SOC3) denetimleri ve raporlamaları

Teknoloji ve siber dayanıklılık yaklaşımı

KVKK/GDPR Uyum, Teknoloji ve Denetim Hizmetleri

Hizmet adı	Kişisel Verilerin Korunması çalışmaları		
Sektör odağı	Tüm sektörler		
Muhtemel süre	▸ **2-3** Hafta – KVKK/GDPR Denetimi ▸ **4-10** Hafta – KVKK/GDPR Uyum Desteği ▸ **2-4** Ay - KVKK Teknoloji Desteği		
Hizmet içeriği	**KVKK/GDPR Denetimi** ▸ Kişisel Verilerin Korunması mevzuatına uygun denetim çalışmaları ▸ Kişisel Veri Koruma Yönetimi Olgunluk Analizleri ve Benchmarklar	**KVKK/GDPR Uyum** ▸ Hukuk, Süreç, Veri Koruma ve Organizasyon unsurları uyum çalışması ▸ İdari ve Teknik Tedbirlere göre hazırlık ▸ Farkındalık eğitimleri ▸ Politika, prosedür ve süreçler	**KVKK/GDPR Teknolojisi (Kurulum, Uyarlama)** ▸ Envanter Yönetimi ▸ Veri Keşfi ve Yönetimi ▸ Veri Saklama ve Silme ▸ Açık Rıza ve Aydınlatma Yönetimi ▸ Mahremiyet Analizi ▸ İhlal Yönetimi ▸ Raporlama

Teknoloji ve siber dayanıklılık yaklaşımı

Eğitim hizmetleri

Hizmet adı	Siber güvenlik farkındalık eğitimleri - online
Sektör odağı	Tüm sektörler
Muhtemel süre	Farklı sürelerde
Hizmet içeriği	▸ Üst Yöneticiler için **2** saatlik eğitim ▸ Bilgi güvenliği yöneticileri için BGYS **2** günlük uygulama eğitimleri ▸ Çalışanlar için **yarım** günlük farkındalık eğitimleri ▸ Bilgi güvenliği farkındalık sınavları ve sonuç raporlamaları

Hizmet adı	KVKK/GDPR farkındalık eğitimleri - online
Sektör odağı	Tüm sektörler
Muhtemel süre	Farklı sürelerde
Hizmet içeriği	▸ KVKK/GDPR Temel Bilgilendirme eğitimi – yarım gün ▸ Uygulayıcılar için İdari ve Teknik Tedbirler eğitimi – **2** gün ▸ Çalışanlar için farkındalık eğitimleri – **yarım** gün ▸ Mahremiyet Etki Analizi eğitimleri – **1** gün ▸ İhlal Yönetimi eğitimi – **yarım** gün

EY | Assurance | Tax | Transactions | Advisory

EY Hakkında
EY bağımsız denetim, vergi, kurumsal finansman ve danışmanlık hizmetlerinde bir dünya lideridir. Anlayışımız ve kaliteli hizmetlerimiz dünya ekonomisi ve sermaye piyasalarında güvenin oluşmasına katkıda bulunmaktadır. EY, güçlü yönetim ekibiyle tüm paydaş gruplarına verdiği sözleri yerine getirmekte ve bu şekilde çalışanları, müşterileri ve içinde yer aldığı diğer çevreler için daha iyi bir çalışma hayatı oluşturulmasında önemli bir rol üstlenmektedir.

EY adı küresel organizasyonu temsil eder ve Ernst & Young Global Limited'in her biri ayrı birer tüzel kişiliğe sahip olan, bir veya daha çok, üye firmasını temsil edebilir. Sınırlı sorumlu bir Birleşik Krallık şirketi olan Ernst & Young Global Limited müşteri hizmeti sunmamaktadır. Daha fazla bilgi için lütfen ey.com adresini ziyaret ediniz.

ey.com/tr
vergidegundem.com
facebook.com/ErnstYoungTurkiye
instagram.com/eyturkiye
twitter.com/EY_Turkiye

İletişim

Ümit Yalçın Şen
EY Türkiye
Şirket Ortağı
Siber Güvenlik Hizmetleri Lideri
umit.sen@tr.ey.com

Feyyaz Burak Baysal
EY Türkiye
Yardımcı Ortak
Teknoloji Risk Hizmetleri Lideri
burak.baysal@tr.ey.com