KPMG

# COVID-19 Döneminde Teknoloji ve Siber Güvenlik

Corona Virüs (COVID-19) gündemi teknoloji ve siber güvenliğin önemini bir kez daha öne çıkardı. Kuruluşlar dijital platformlar, uzaktan erişim, alternatif iletişim kanalları, güvenlik ve altyapının devamlılığı anlamında zorlu bir sınav veriyor. Teknoloji ve güvenlik yöneticilerinin bu alanlardaki güncel riskleri ve aksiyonları yakın takip etmeleri gerekiyor.

Mart 2020

kpmg.com.tr

# Covid-19'in teknoloji ve güvenliğe etkisi

COVID-19 virüsünün tespit edildiği günden itibaren, süreç boyunca kendimizi virüsten korumak için yapılması gerekenler hakkında sürekli olarak bilgilendirildik. Salgın sırasında kuruluşların çalışanlarının virüsten etkilenmemesi ve salgını oluşabilecek en az zararla atlatmak adına, çalışanlara evden çalışma imkanı ve uzaktan erişim yetkisi verildi. Bilgi teknolojileri altyapısı ve siber güvenliğin yaşanan bu süreçte yine önemli konulardan birisi olduğunu gözlemliyoruz. Bu alanlardaki önlemleri soruları ve önlemleri sıraladık.


# Önerilen aksiyonlar


- Çalışanların uzaktan çalışma için gerekli mobil cihazlara ve erişim imkanına sahip mi?
- Ağ, VPN, portal ve gateway altyapılarının uzaktan çalışmayı taşıyabilecek kapasitede ve yedekli olduğunuz test ettiniz mi?
- Çalışanlar dışında uzaktan erişim ihtiyacı duyan (tedarikçiler, müşteriler, ortaklar) tarafları değerlendirdiniz mi?
- Uzaktan erişim için uygun kimliklendirme mekanizmasına (sertifika, anahtar veya şifre) sahip misiniz?
- Çalışanların güvende olmasını takip edecek olanaklara sahip misiniz?
- Video/telekonferans olanakları kısıtlıysa, lisans ve kapasite genişletilebilir mi?
- Uzaktan erişim modelinde, ana ve idari uygulamalara erişimin yeterli olduğunu test ederek belirlediniz mi?


- Artan müşteri talepleri için dijital kanalların ve platformların kapasitesini değerlendirdiniz mi?
- Müşteriler için alternatif tedarik ve hizmet yöntemlerini değerlendirdiniz mi?
- Çağrı merkezi operasyonlarınızın sürekliliğini değerlendirip uzaktan erişim yöntemlerini uyguladınız mı?
- Yükün dengelenmesi için mevcut bulut çözümlerinin kapasitesini ve bunları artırmayı değerlendirdiniz mi?


- Kritik teknoloji tedarikçilerinizi, bunlarla ilgili riskleri ve altnernatifleri belirlediniz mi?
- Tedarikçilerin hizmet verememesi durumunda iç kaynakların devreye alınması söz konusu mu?
- Tedarikçilerle sözleşmeleriniz ve iletişim kanalınız gerekli eskalasyonu yürütmenize ve aksiyonları almanıza müsaade ediyor mu?
- Tedarikçileriniz içerisinde finansal kararlılığı bozulan kuruluşlar var mı?

# Önerilen aksiyonlar


- Mevcut durumda veya salgının binanıza yayılması durumunda, veri verkeziyle ilgili alternatif erişim ve operasyon yöntemleriniz mevcut mu?
- Sistemlerin kesinti yaşaması ihtimaline karşı felaket kurtarma merkezine sahip misiniz?
- Alternatif lokasyon ve sistemlerinizden devam etme yönteminiz ve hızınız nedir?
- Veri merkezi operasyonu için tedarikçilere ve anahtar personele bağımlı mısınız? Olası alternatiflerinizi değerlendirdiniz mi?


- Anahtar BT personelinin seyahat edememesi, hasta olması veya çok kısıtlı olması durumunda alternatif önlemleriniz nelerdir?
- Bu bağımlılığa karşı önlemleriniz nelerdir, örneğin acil durum erişim prosedürleriniz mevcut mu?
- Güvenlik ekibinin veya bilgi güvenliği yöneticisinin erişilemez olması durumunda güvenlik işlemlerini ve kararlarını kimlerin yürüteceği belirlendi mi?


- Çalışanların sağlığına ilişkin veriler özel nitelikli kişisel veri olarak tanımlanıp korunması için önlemler alınıyor mu?
- Çalışanların takibi için toplanılan ve izlenen araç, lokasyon, iletişim bilgiler, vb benzeri kişisel verilerin gizliliği sağlanıyor mu?


- Çalışanları COVID-19'a ilişkin artan siber güvenlik vakalarıyla ilgili bilgilendirdiniz mi?
- Çalışanlar oltalama saldırılarına karşı almaları gereken önlemlerin farkında mı?
- Bu dönemde gerçekleşebilecek siber saldırı senaryolarına karşı vaka yönetimi süreçleriniz mevcut mu?
- Güvenlik vakalarının izlenebilmesi için loglama ve izleme altyapılarınız mevcut mu, bu sistemlerin işlerliğinden emin misiniz?
- Çalışanların acil yetki ve erişim taleplerini bildirebileceği süreçlere sahip misiniz?
- Kullanıcı şifre politikalarının yeterince güçlü olduğundan emin misiniz?
- Uzaktan çalışma modelinde mobil cihazların ve iletişim kanallarının şifreli olmasını temin ettiniz mi?
- Anti-virüs tanımları güncel mi ve peryodik olarak taramalar yapılıyor mu?


- Servis masası ve operasyon çalışanlarının uzaktan/evden çalışma düzenlemeleri mevcut mu?
- Acil durumlarda sahada ve yerinde müdahale edebilecek kişiler belirlendi mi?
- İkinci seviyedeki müdahale işlemleri için gerekli personel ve tedarikçiler erişilebilir durumda mı?


- Verilerin yedeklerinin güncel ve erişilebilir olduğundan emin misiniz?
- Olası bir fidye yazılımı vakasına karşı masaüstü ortamlar dahil yedeklemelerin alındığından emin misiniz?
- Teknoloji ekiplerinin projelerini, faaliyetlerini ve operasyonlarını önceliklendirerek en kritik alanlarda çalışmalarını temin ettiniz mi?

# İletişim:

**Servet Gözel**
Direktör,
Siber Güvenlik Lideri,
Bilgi Teknolojileri Danışmanlığı
servetgozel@kpmg.com

**Detaylı bilgi için:**
KPMG Türkiye
Clients & Markets
tr-fmmarkets@kpmg.com

**İstanbul**
İş Kuleleri Kule 3 Kat 1-9
34330 Levent İstanbul
T: +90 212 316 6000

**Ankara**
The Paragon İş Merkezi Kızılırmak Mah.
Ufuk Üniversitesi Cad. 1445 Sok. No:2
Kat:13 Çukurambar 06550 Ankara
T: +90 312 491 7231

**İzmir**
Heris Tower, Akdeniz Mah. Şehit Fethi Bey
Cad. No:55 Kat:21 Alsancak 35210 İzmir
T: +90 232 464 2045

**kpmg.com.tr**
**kpmgvergi.com**