Independent Advisors & Accountants

Tax-IA Bulletin

No : 2020-35

Tarih : 5 Nisan 2020

Konu : COVID-19 Bilgi Teknolojilerinde Riskler & Fırsatlar

Corona Virüs Salgınının

BT Riskleri ve Fırsatları Açısından Değerlendirilmesi

COVID 19 virüsünün sebep olduğu salgın, iş yapış şekillerimizi hiç beklemediğimiz bir anda ve çok kısa bir sürede değiştirdi. Daha öncesinde- en azından 3. Sanayi devrimi kabul edilen 1960-70'lerden bu yana- benzer bir krizle karşılaşılmamış olması içinde bulunduğumuz durumu özel kılıyor. Bu yazıda BT uzmanı sayın Önder Devrim Erol ile soru cevaplı bir şekilde Covid 19 dünyasında bilgi teknolojilerinde riskleri ve fırsatları konuştuk. Keyifli okumalar dileriz hepinize.

1. Mevcut Durumun Farkı Nedir?

Mevcut durum, daha çok siber güvenlik saldırıları, deprem, su baskını gibi olumsuzlardan kaynaklı iş süreklilik planları ve güvenlik politikaları olan kurumların pek de hazırlıklı olmadıkları bir süreç.

Burada hazırlıklı olmamak, daha çok ne ile karşı karşıya kalındığının net olmamasından kaynaklanıyor. Örneğin bir siber saldırı kaynaklı kesinti ya da aksama olması durumunda neler yapılacağı biliniyor. Kurumunuzda bu konuda yetkin çalışan olmasa da piyasada bu alanda yetişmiş pek çok kişi ve kurum var, gerektiğinde bunlardan destek almanız mümkün. Oysa virüs salgını nedeniyle kriz yönetimi tecrübesine sahip kişilere rastlamak kolay değil.

İkinci ayırt edici durum ise yaygınlık. Belli bir firma, sektör ya da coğrafi alan değil, tüm dünya aynı sorunla karşı karşıya. Dünyanın her ülkesinde bankacılıktan havacılığa tüm sektörler daha önce karşılaşmadıkları bir riskle aynı anda karşı karşıyalar. Dolayısıyla sağlık sektöründeki kaynak kıtlığı ve talep fazlalığı aslında bilişim sektörü için de geçerli.

Bu kısa değerlendirmemizde bilgi sistemleri açısından içinde bulunduğumuz durumun risklerini, yapabileceklerimizi ve son olarak da olası fırsatları değerlendirmeye aldık.

2. Corona Salgınının BT Açısından Riskleri Nelerdir ve Önlemleri Nasıl Olmalı?

a. ***İş sürekliliğinin sağlanması:*** Tüm alanlarda olduğu gibi bilgi sistemleri özelinde de en önemli konu iş sürekliliğinin devam ettirilmesidir. Bunu sağlayabilmek için en başta çalışan sürekliliğinin sağlanması geliyor. Bu da çalışanların sağlığının korunması ile mümkün. Bu konuda her kurum kendi çalışanları için önlemler alıyor. Ancak, bunun nasıl olması gerektiği bu yazımızın konusu değil. Bu nedenle bizim için yapılacaklar listesinin başında, iş süreklilik planlarının hazır ve uygulanabilir olması bulunuyor. Bilgi sistemleri anahtar personelinin ve bu kişilerin yedeklerinin atanmış olması önemli. Olağanüstü şartlarda geçici de olsa olağanüstü yetkilendirmeler ya da yetki çatışmaları ile karşılaşmak mümkün. Bu tip durumlarda yetkilendirmelerin kayıtlı olması ve şartlar iyileştiğinde en kısa sürede eski duruma dönülmesinin atlanmaması gerekiyor.

b. ***Üçüncü taraflardan alınan BT hizmetlerinde aksama:*** Firmaların kendi bünyeleri dışından sağladıkları BT hizmetlerine ilişkin risklerin değerlendirilmesi ve alınan hizmetlerin alternatiflerinin göz önünde bulundurulması da dikkat edilmesi gereken bir diğer husus. Alınan hizmetin ne kadar hayati olduğu ile ilgili olarak, yaşanacak aksamanın kurumun sürekliliğine etkisinin değerlendirilmesi ve aksiyonların buna göre belirlenmesi önem arz ediyor. Bu konuya ek olarak, kuruma erişim sağlayan üçüncü tarafların izlenmesi ihmal edilmemeli. Kendi kurumumuzda ortaya çıkan alternatif kaynak ihtiyacı (personel, donanım, yazılım, vb.) aynı şekilde hizmet aldığımız firmalarda da ortaya çıkabilir. Bizim kurumumuza her zaman erişim sağlayan kişilerden başka kişiler ya da uygulamalar ile ya da alt yükleniciler tarafından erişim sağlanması söz konusu olabilir. Bu durumların da göz önünde bulundurulması faydalı olacaktır.

c. ***(Evde Kal Dünya) Uzaktan çalışmanın getirdiği riskler:*** Çalışanların enfeksiyon riskini azaltmak için pek çok kurum bu dönemde uzaktan çalışma yöntemini uygulamaya başladı. Aslında uzun süredir mevcut olan bu uygulama, dünya genelinde hiç olmadığı kadar yaygınlaştı demek daha doğru olur. Çalışanlara uzaktan erişim verilirken, erişime açılacak ortamların gözden geçirilmesi faydalı olacaktır. Her türlü uzaktan erişim mutlaka loglanmalı, mesai saatleri dışında sağlanan erişimlere ayrıca dikkat edilmelidir.

   Uzaktan erişimlerde dikkat edilmesi gereken bir başka konu ise rol ve kimlik yönetimi. Özellikle kişisel veriler ya da müşteri bilgileri gibi daha hassas alanlara erişimlerin kısıtlanması, gerekli yerlerde ikinci bir doğrulama (otantikasyon) istenmesi seçeneği göz önünde bulundurulmalı.

d. ***BT kaynaklarının yönetimi*** de bu hassas donemde önem kazanıyor. Uzaktan erişime geçişle birlikte kurum kaynaklarının önemli bir kısmının bu alana aktarılması, kurumda normal şartlarda yapılması gereken zaruri işlemleri aksatabilecektir. Örneğin gerekli yamaların geçilmesinin ertelenmesi ya da güncellemelerin geciktirilmesi gibi.

Benzer şekilde BT yardım masası çalışanlarının da ağırlıklı olarak uzaktan erişim sağlayan personele destek vermeleri durumunda diğer alanlardan gelen taleplerin yerine getirilmelerinde aksamalar yaşanabilecektir. Kurumun bilgi sistemlerindeki insan kaynağı da dahil tüm kaynaklarının ne yöne kanalize edileceğinin kurum tarafından önceliklendirilmesi bu noktada çok önemli hale gelmektedir. Çünkü kurumların bilgi sistemleri, kurumun hedeflerine ulaşmada ona destek olan en önemli varlıklarındandır. Bu noktada bilgi işlem bölümlerinin tek başına inisiyatif almalarını gerektirmeyecek şekilde üst yönetim tarafından gerekli yönlendirmeler yerine getirilmelidir.

e. ***Fiziksel güvenlik:*** Yukarıda sayılanlara ek olarak uzaktan erişimlerde fiziksel güvenliğin gözetilmesi gereklidir. Örneğin erişim sağlanan cihazlarda verilerin şifreli saklanması kayıp ya da çalıntı durumlarında verinin kötü niyetli kişilerin eline geçmesini engelleyecektir.

Bağlanılan ağların herkese açık olmaması ve mutlaka VPN kullanılması ihmal edilmemesi gereken hususlardır. Aksi durumda, kurumla iletişiminizde araya girilebilir (*Man in the Middle*), kimliğiniz ve verileriniz ele geçirilebilir, kurumunuza erişim sağlanabilir, sonuç olarak kurumunuz ve siz zarar görebilirsiniz.

Nitekim COVID 19 salgını sonrası "Corona" kelimesi içeren binlerce alan adına kayıt işlemi gerçekleştirildiği ve bu web sitelerinin önemli bir kısmının zararlı içerik barındırdığı ortaya çıkmıştır *(https://www.domaintools.com)*. Salgından çıkar elde edebilmek için çalışanlara coronavirüs ile ilgili bilgi veriyormuş gibi görünen oltalama (phishing) e-postaları göndererek kimlik bilgileri istenmekte, eposta içeriğindeki bağlantılar ya da ekteki dosyalar yoluyla sistemlere zararlı yazılımlar bulaştırabilmektedirler. Bu olumsuzlukların önüne geçmek için çalışanlara temel bir siber farkındalık eğitimi verilmesi faydalı olacaktır. Bu şekilde zararlı e-postalar fark edilerek kurumsal ve kişisel verilerin güvenliği artırılabilir. Artık biri ya da birkaçı hemen her kurumda olan anti virüs, firewall, WAF, vb. güvenlik önlemlerine tek başına güvenmek çalışanların bilinçli olmadığı durumda, üstelik mevcut şartlarda maalesef geçerli bir anlayış değil *(https://siberbulten.com)*.

Daha nitelikli saldırılarda ise sizin bağlantılı olduğunuz ya da çalıştığınız firmadan geliyormuş gibi size özel e-posta ya da uzaktan bağlantı talebi gelmesi durumu söz konusu olabilmektedir.

3. Corona Salgınının Ortaya Çıkardığı Fırsatlar Var mıdır?

Risklere ve alınabilecek önlemlere kısaca değindikten sonra bu durumun getirdiği fırsatlara da yer vermek istiyoruz.

a. ***Bulut hizmetlerinin ön plana çıkması:*** Dünyada tedarik zincirlerine bağlı üretim sekteye uğrarken, bulut esaslı yazılım hizmetlerinde artış görülüyor. Her şeyden önce, kurumların uzaktan erişimle iş yapmaya ağırlık vermesi, bulut bilişim tarafında hiç olmadığı kadar talep artışı hatta patlaması yaratmış durumda. Örneğin Microsoft bulut hizmetlerinde salgın ortaya çıktıktan sonra %775 artış yaşanmış (*https://azure.microsoft.com*). Benzer şekilde, Zoom, Slack, Microsoft Office365, Atlassian gibi uygulamalar da uzaktan erişim talebinin artması neticesinde talep artışı yaşayan firmalar. Nitekim önümüzdeki birkaç yıllık dönemde de bulut bilişim ve iletişim yazılımları, bilişim tarafında yatırım çekecek alanlar olarak görülüyor (*https://go.forrester.com/*).

b. ***Afet durumları için özel uygulamalar:*** Virüs ile enfekte olmuş kişilerin konumlarını paylaşan, bu şekilde diğer insanları uyarmayı amaçlayan yazılımlar, salgın durumlarda kullanılmaya başlandı. Kişilerin konum bilgilerinin kullanılarak hem önleyici hem de tespit edici faaliyetler için bu bilginin kullanım imkanının doğması, bu alandaki uygulamalar için yeni faaliyet alanları anlamına geliyor. Hükümetler de bu tür uygulamalara imkân tanıyacak düzenlemeleri yapmaya başladılar (*https://www.news18.com/*). Ülkemizde de 26.3.2020 tarihinde yayımlanan 7226 sayılı Kanun (*https://www.resmigazete.gov.tr/eskiler/2020/03/20200326M1-1.htm)* ile afet ve acil durum halleri ile 112 çağrı merkezine yapılan aramalarda abone ve konum bilgilerinin Bilgi Teknolojileri ve İletişim Kurumu tarafından karşılanacağı hususu düzenlendi. Kişisel verilerin paylaşımı ile bu uygulamaların faaliyetlerine imkân tanımak da kişisel verinin kapsamı ve kullanımı için yeni tartışmalar getiriyor.

Sonuçta, geçirmekte olduğumuz kriz sonrasındaki toparlanma dönemi kriz döneminden muhtemelen daha uzun süreceği için, iyi yönetilmiş bir krizden çıkarılan dersler ve kriz esnasında kurulan ilişkiler, toparlanma döneminde ve olası yeni bir krizde de işletmeye paha biçilmez değer katacaktır.

Saygılarımızla.

Independent Advisors | BT & Tax
Mecidiyeköy Mahallesi Şehit Ahmet Sok. Ada Residence No: 6-10/51, Kat: 3
34381 Şişli İstanbul Tel: +90 212 211 11 10

Ankara: Kent İş Merkezi, Mustafa Kemal Mahallesi, 2152 Cadde, No:2 Kat:9 Daire No:18
Çankaya/Ankara, 06510 Tel: +90 312 446 92 05
www.ia.com.tr