



Değerli müşterilerimiz;

Bu ay sizler için hazırlamış olduğumuz bültenimizde; bilgi ve bilgi sistemleri dünyasının bir gerçeği olan **“Siber Riskler”** ve Siber Risklerin sonuçları ve bilgi güvenliğine dair önemli bilgilere yer vermek istiyoruz.



➤ **Siber Riskler Nelerdir?**

İster mobil cihazlarında, bilgisayarlarında isterse sunucularında veya internette elektronik veri kullanan herhangi bir şirket, bu risklerle karşı karşıyadır.

Siber Riskler, bir dizüstü bilgisayar üzerindeki bilgi kaybından, internet bilişiminin oluşturduğu tehditlere kadar geniş bir yelpaze oluşturmaktadır. İşletmeler, internet ortamındaki varlıklarının silinmesi veya kesintiye uğratılmasıyla karşı karşıya kalabilmektedirler.

Kuruluşlar eskiden, sadece fiziksel varlıklarını koruma amaçlı yatırım yaparken, artık dikkatlerin ağ ve sistem korumalarına da odaklanması gerektiği göz ardı edilmemelidir.

➤ **Siber Riskler neden bu kadar önemlidir?**



Siber Risklerin teşkil ettiği tehdit, artık bir şirketin varlıklarına yönelik fiziksel tehditler kadar somuttur ve ciddi artçı etkilere sahiptir.

Kurumsal şirketlerin bilişim sistemlerine bağımlılığı arttıkça açıkları da aynı şekilde artmaktadır. Bilişim sistemlerine çok bağlı olan bu işletmeler herhangi bir bilgisayara gelecek zarar ve güvenlik ihlalleri ile şirket çapında ciddi mali kayıp tehlikeleriyle karşı karşıyalar.

➤ **Bir işletmenin Siber Risklere maruz kalması sonrası yaşanabilecek sorunlar;**

Veri Sızıntısı; Dijital veriler, şirketin sisteminden kaybolur veya sızdırılır. Bu kayıp, bir kişisel bilgisayar, dizüstü bilgisayar, mobil cihaz veya tablet üzerinden gerçekleşebilir.

Bilgi İşlem Krizi; Bilgi işlem departmanının, bir yandan sorunla başa çıkarken diğer yandan da olağan akışında işi yönetmesi gerekmektedir. Bu bir sızıntı mı, yoksa kayıp mı, yoksa şirket hacklendi mi? Veriler nasıl çalındı veya kayboldu? Verilen şu an nerede? Sunucunun kapatılması gerekecek mi? Yedek sunucu yazılımına ihtiyaç var mı? vb. sorunlar ortaya çıkacaktır.



Halkla İlişkiler; Sızıntı haberleri, özellikle bu sosyal medya çağında hızla yayılmaktadır. Şirkete olan güven, olayın üzerinden saatler geçmeden azalabilir. Müşterilere verilerin çalındığı



GÖZETMEN

SİGORTA BROKERLİĞİ

söylenmeli mi? Başka kime bilgi verilmeli? Bunu yapmanın en kolay yolu ne? Güveni geri kazanmak ve şirketin itibarını korumak, hızlı harekete geçmeyi ve özenle yönetilen bir halkla ilişkiler müdahalesini gerektirmektedir.

Finansal Kriz; Finansal etkilerin uzantıları oluşmaya başlamıştır. Veri ihlalleri için düzenleyici cezalar olabilir. Şirketinizdeki sızıntı yüzünden, veri kaybı sebebiyle kendi müşterilerine tazminat ödemek zorunda kalan 3. şahıslar bu tazminatı sizden talep edebilirler. İşletme finansal olarak da işleyemeyecek durumda olduğundan, kar kaybı da söz konusu olabilecektir.

Yönetim Krizi; Bir siber kriz sonrası, yönetimin ve şirketin itibarı ciddi şekilde tehlikeye girebilir.

➤ **Siber Riskler (Veri Koruma Sigortası) nedir?**



Veri Koruma Sigortası; siber risklerin belirgin ve daha az belirgin sonuçlarını teminat altına alarak şirketlerin, domino etkisinin bir parçası olarak her şeyin “devrilmeyeceğini” bilerek günlük işlerine devam edebilmelerini sağlar.

Bu sigorta ile; verinin sızıntısı, kaybı veya ihlalinin sadece olası etkilerini değil aynı zamanda geleneksel sigorta teminatı ile profesyonel danışmanlık hizmetlerini birleştirerek; itibara ve bilgi işleme etkisini de azaltmaya yardımcı olmaktadır.

➤ **Veri Koruma Sigortası'nın Faydaları ve Kapsamı**

Kriz Yönetimi; Veri Koruma Sigortası, itibar kaybının yönetilmesine yardımcı olur. Kriz Yönetimi ile işletmeye aşağıda belirtilen hizmetler verilir.

Şirketin itibarının onarılması, Kişisel itibarı onarma, yapılacak bildirim ve izleme masrafları.

Veri Sorumluluğu; İster sigortalı ister sigortalının dış kaynak firması neden olmuş olsun, kişisel veya kurumların ihlali ile bağlantılı zararları karşılanmaktadır.

Ağ Güvenliği; Aşağıdakilerle bağlantılı zararlar ve savunma masrafları teminat kapsamındadır.

- * Bir üçüncü şahsın verilerine virüs bulaşması,
- * Sigortalının yetkisi dışında bir üçüncü şahsın verilerine erişmesiyle sonuçlanan bir fiili veya ihmali
- * Bir sistem kodunun elektronik olmayan yöntemlerle çalınması,
- * Kişisel bilgiler içeren donanımın çalınması
- * Bir çalışanın fiilleri nedeniyle verilerin ifşa olması.



İdari Yükümlülükler; Bir veri koruma sigortası soruşturması ile bağlantılı hukuki danışmanlık masrafları ile bir veri koruma düzenleme makamının uyguladığı sigorta edilebilir para cezaları teminat altındadır.

Gözetmen Sigorta Brokerliği olarak; Siber Riskler(Veri Koruma) Sigortaları veya diğer özel sigorta ihtiyaçlarınız ile ilgili her türlü konuda sizlere destek olabileceğimizi belirtmek isteriz.

Saygılarımızla.

HER TÜRLÜ SİGORTA İHTİYACINIZ İÇİN BİZİ ARAYABİLİRSİNİZ.