POTANSİYEL VERİ GÜVENLİĞİ İHLAL PROTOKOLÜ

A. AMAÇ

İşbu protokol, bir veri ihlali halinde Gedik Yatırım Menkul Değerler A.Ş.'nin mevcut teknik, idari ve fiziki tedbirlerini belirlemek amacı ile hazırlanmıştır. Gedik Yatırım Menkul Değerler A.Ş.'nin itibar ve güvenliğinin zedelenmesinin önüne geçilmesi ve doğabilecek zararların Gedik Yatırım Menkul Değerler A.Ş.'yi etkileyen sonuçlarının en aza indirilmesi amaçlanmaktadır.

Veri ihlalleri her durumda mümkündür. Veri güvenliğinin en üst düzeye taşınmasında dahi bir veri ihlali söz konusu olabilir. Böyle bir durumda atılacak adımların belirlenmesi ve uygulanması önem arz etmektedir.

Bu protokol, Gedik Yatırım Menkul Değerler A.Ş.'nin zaman, senaryo ve teknolojiden bağımsız olarak veri ihlali durumunda izlemesi gereken adımları ortaya koymayı amaçlamaktadır.

B. VERİ İHLALİNE KARŞI ŞİRKETİN SORUMLULUKLARI

Aşağıda belirtilen önlemler alınarak veri ihlallerinin mümkün olduğunca önüne geçilmesi hedeflenmektedir:

1. Veri ihlali doğurabilecek senaryolar listelenmeli ve veri ihlali durumunda belirlenen her senaryo için yapılacaklar planlanmalıdır.

2. Veri ihlali durumunda, konuyu sonlandırabilecek yetkili kişi veya kişiler belirlenmeli, bu kişilerin görev ve yetki tanımları yapılmalıdır.

3. Veri ihlalinin önüne geçilebilmesi için Acil Durum Eylem Planı Kontrol Listesi'nde yer alan adımlar izlenmelidir.

4. Veri ihlalinin çıkış noktası belirlenmeli, deliller toplanmalı ve korunmalıdır.

5. Somut olaya uyarlanarak kullanılabilecek taslak ihlal bildirimleri hazırlanmalıdır. Kişisel Verilerin Korunması Kurulu tarafından öngörülen bir metin yayımlanması halinde ise yayımlanan metin esas alınmalıdır.

6. Veri ihlali sonucu Kişisel Verilerin Korunması Kurumu gibi kurumlara hukuken bildirim yükümlülüğü ortaya çıkmış ise gerekli bildirimler yapılarak bu yükümlülük yerine getirilmelidir.

7. Veri ihlali ile Gedik Yatırım Menkul Değerler A.Ş. bünyesinde bulunan kişisel veriler üzerinde herhangi bir işlem (ele geçirme, silme, güncelleme gibi) yapıldığına kanaat getiriliyorsa, 6698 sayılı Kişisel Verilerin Korunması Kanununun ilgili hükümleri uyarınca veri sahipleri konu ile ilgili derhal bilgilendirilmelidir.

8. İhlal hakkında iç birimlerin yetersiz olduğu düşünülüyorsa ilgili gizlilik sözleşmeleri yapılarak gerekli olan teknik ve hukuki destek alınmalıdır.

C. VERİ GÜVENLİĞİ İHLALİ DURUMUNDA YAPILACAKLAR

Veri ihlali ile karşılaşan veya veri ihlalini tespit eden çalışanın vakit kaybetmeden departman yetkilisini ve Gedik Yatırım Menkul Değerler A.Ş. KVKK Yönetişim Komitesi'ni bilgilendirmesi gerekmektedir. Sonrasında departman yetkilisi ve Gedik Yatırım Menkul Değerler A.Ş. KVKK Yönetişim Komitesi ihlalin yaratabileceği sonuçları değerlendirerek ilgili görebilecekleri kişi veya departmanlara konuyu taşımalıdır.

İhlal sırasında bilgilendirilmek üzere tespit edilen "Müdahale Ekibi"nde bulunan irtibat kişileri arasında aşağıda belirlenen kişiler yer almalı ve işbu prosedürde yer alan tüm durumlarda bu irtibat listesi kullanılmalıdır:

a. En az bir Gedik Yatırım Menkul Değerler A.Ş. Yönetim Kurulu personeli,

b. Hukuk çalışanı,

c. BT çalışanı,

d. İnsan Kaynakları çalışanı.

İhlal kapsamında Gedik Yatırım Menkul Değerler A.Ş.'nin e-posta sisteminin de ihlalden etkilendiği düşünülüyorsa, daha fazla veri ihlalinin ortaya çıkmaması ve ihlalin sonlandırılabilmesi adına yapılacak bildirimler telefon yolu ile veya yüz yüze yapılmalıdır.

1. İhlalin Değerlendirilmesi

İhlal değerlendirilirken yapılacak her türlü işlem kayıt altına alınmalı, kayıt esnasında aşağıda belirtilen detaylar dikkate alınmalıdır. Bu detayların yetersiz kaldığının düşünüldüğü durumlarda veri ihlalinin durumu değerlendirilerek ek değerlendirmelerde bulunulabilir. Kayıt altına alınması beklenen işlemler başında aşağıdakiler gelmektedir:

a. İhlalin hangi verileri ve sistemleri etkilediği

b. Yapılan işlemlerin saati ve tarih bilgileri

c. İhlal ile ilgili olabilecek kişiler (olayı fark eden, önlemleri gerçekleştirmeye çalışan, kaydı oluşturan kişiler)

d. İhlalin değerlendirilmesi ve sonlanması için atılan adımlar

2. Veri İhlalinin İncelenmesi ve Hasarı En Aza İndirme Süreçleri

İlgili birimin veri ihlalinin nasıl gerçekleştiğini belirlemesinin ardından, ihlalin tekrar yaşanmaması ve zararın büyümemesi için aşağıda listelenen önlemler alınmalıdır. Bu önlemlerin yetersiz kaldığının düşünüldüğü durumlarda, Gedik Yatırım Menkul Değerler A.Ş. ek önlemler de almakla yükümlüdür.

a. Veri sahipliği fiziki veya elektronik olarak kaybolmuş bir veri söz konusu ise, bu verilerin güvenliği Gedik Yatırım Menkul Değerler A.Ş. tarafından tekrar sağlanmalıdır.

b. Kolluk kuvvetlerine haber verilmesi uygun ise vakit kaybetmeden bu başvuru yapılmalıdır.

c. Verilerin bulunduğu ortamlara giriş çıkışlar sınırlandırılmalıdır.

d. Fiziksel ortamda veya bilgisayar ortamında tutulan veriler fiziki olarak ihlale uğramış ise fiziki ortama ait giriş – çıkış ve kamera kayıtları korunmalıdır.

e. Bilgisayar ortamında tutulan veriler ihlale uğramış ise mevcut denetim izi kayıtları oluşabilecek herhangi bir müdahaleye karşı korunmalıdır.

Gedik Yatırım Menkul Değerler A.Ş., yapılan inceleme ve analizler sırasında aşağıda listelenen maddelerin üzerinden ilerleyerek veri ihlali ile ilgili aksiyon almalıdır:

a. Veri ihlali sebeplerinin değerlendirilmesi,

b. Veri ihlalinden etkilenen veri sahiplerinin belirlenmesi

c. İhlale uğrayan verilerin ne gibi amaçlar için kullanılacağının tespit edilmesi

d. Risk altındaki diğer sistemlerin belirlenmesi

Bu süreçte veri ihlalini inceleyen sorumlu kişi mutlaka Müdahale Ekibi'nde bulunan BT personelinden destek almalıdır. BT personelinin yetersiz kaldığı durumlarda, BT Departmanı'ndan veya dış kaynaklardan destek alınabilir.

Veri ihlali incelenirken tutulacak olan tüm belgeler gizli olmalıdır ve belgeler üzerinde "Gizli ve İmtiyazlıdır" ifadesi bulunmalıdır.

3. Veri İhlali Sonrası Yapılacak Bildirimler

Veri ihlali sonrasında Gedik Yatırım Menkul Değerler A.Ş., kişi ve kurumları bilgilendirmekle yükümlüdür. Bilgilendirme verilerin sahibi kişi ise direkt olarak gerçek kişilere, başka bir şirketin (iş ortakları veya diğer şirketler) verileri ise ilgili şirkete yapılmalıdır.

Bildirim yapılması hukuken gereklidir ve kamu ilişkileri için önem taşımaktadır. Bu sebeple yapılacak olan bildirim planlı olmalı ve bildirim metni ilgili departman yetkilisi tarafından hazırlanmalıdır. Hazırlanan bildirim metni Hukuk Departmanı'nın incelemesinin ardından ilgili yerlerle paylaşılmalıdır. Bildirim içerisinde aşağıdaki başlıklara yer verilmeli, bu başlıkların yeterli olmadığı düşünülen durumlarda Hukuk Departmanı'nın bilgisi dâhilinde ekleme yapılmalıdır:

a. Veri ihlalinin açıklanması,

b. Veri ihlalinden kimlerin etkilendiği,

c. Alınan önlemler,

d. Gedik Yatırım Menkul Değerler A.Ş.'nin veri ihlalinden etkilenen kişilere nasıl yardımcı olacağı,

e. İhlalden etkilenen kişilerin Gedik Yatırım Menkul Değerler A.Ş.'ye ulaşabilecekleri iletişim bilgileri.

Analizler sırasında ihlale konu olan verilerin başka bir şirkete ait olduğu tespit edilirse, ilgili şirkete ihlal bildirimi yapılmalıdır. Bu bildirim planlanırken aşağıdaki şartlar dikkate alınmalıdır:

a. Bildirim, belirlenmiş olan ilgili şirket irtibat kişisi veya kişilerine yapılmalıdır. Bu kişilere ulaşılamaması durumunda Gedik Yatırım Menkul Değerler A.Ş. Hukuk Departmanı'na danışılmadan farklı bir kişiye bildirim yapılmamalıdır.

b. Bildirim iletişim kanalı veri ihlali ile ilişkili olacak şekilde Müdahale Ekibi tarafından belirlenmelidir.

D. BİLGİ TEKNOLOJİLERİ ACİL DURUM EYLEM PLANI KONTROL LİSTESİ

1. Bilgi Teknolojileri Acil Durum Eylem Planı Kontrol Listesinin Amacı

İşbu Bilgi Teknolojileri Acil Durum Eylem Planı Kontrol Listesi ("Kontrol Listesi"), Gedik Yatırım Menkul Değerler A.Ş. çalışanlarının bilgi teknolojileri ("BT") sistemlerinde bir zafiyet yaşanması durumunda izleyecekleri adımlara rehberlik etmek amacıyla hazırlanmıştır. BT sistemlerinde yaşanan zafiyetler kasten ya da sehven yapılan hatalar sebebiyle veya sürekli değişen saldırı teknikleri kullanılarak meydana gelmektedir. Kontrol Listesi, herhangi bir zafiyetin önlenmesi veya zafiyetin tam olarak tespit edilmesi gibi bir amaç taşımamaktadır.

Belirli aralıklarla gözden geçirilmeli ve güncellenmelidir.

2. Kontrol Listesi

1. Vaka yaşandı mı veya vaka yaşandığından şüpheleniliyor mu?
2. Vaka devam ediyor mu?
3. Vakanın kişisel verilere bir etkisi oldu mu?
4. Vakayla ilgili aksiyonları alacak bir kriz masası kuruldu mu?
5. Etkilenen sistemler kurum ağından izole edildi mi?
6. Etkilenen sistemlerin tutulduğu sunucu/pclerin kapanması engellendi mi?
7. Aşağıdaki bilgiler kayıt altına alındı mı?

7.1. Vakayı tespit eden kişi veya alarmın kaynağı

7.2. Vakaya ait ilk tespitin tarih ve saati

7.3. Vaka hakkında temel bilgiler

7.4. Hangi kişilerin veya sistemlerin etkilendiği

7.5. Dâhil olan kişilerin veya sistemlerin konumu

7.6. Vakanın nasıl tespit edildiği

8. Etkilenen sistemin önem derecesi kritik mi?
9. Hedef olan sistem(ler)in:

9.1. Adı

9.2. İşletim sistemi

9.3. IP adresi

9.4. Ağ üzerindeki konumu

9.5. Fiziksel konumu

9.6. Kullanım amacı

10. Hangi sistemler veya veriler tehlike altında?
11. Tehlike altındaki sistemlerin veya verilerin kategorisi nedir?
12. Saldırının kaynağı kurum içi mi, kurum dışı mı?
13. Vakanın soruşturulması sırasında aşağıdaki çalışmalar yapıldı mı?

13.1. Sistem loglarının incelenmesi

13.2. Uygulama loglarının incelenmesi

13.3. Loglardaki boşlukların denetlenmesi

13.4. Varsa firewall loglarının incelenmesi

13.5. Varsa VPN erişim loglarının incelenmesi

13.6. Varsa router loglarının incelenmesi

13.7. Uygulama loglarının kontrol edilmesi

13.8. Etkilenen sistemlerin memory dump dosyalarının alınması ve incelenmesi

13.9. Vakayı tespit eden ve vakadan etkilenen çalışanlarla mülakatların yapılması ve vakayla ilgili mümkün olduğunca detaylı bilgi alınması

13.10. Elde edilen deliller için delil zinciri ("Chain of Custody") dokümanı hazırlanması

13.11. Elde edilen verilerin sadece erişim yetkisi olan kişilerin ulaşabildiği, giriş-çıkışları kontrol altında olan bir alanda tutulması

14. Vakanın kuruma finansal etkisi tespit edildi mi?

15. Kişisel veriler etkilendiyse verileri etkilenen kişiler ve etkilenen veriler tespit edildi mi? Tespitler doğrultusunda veri öznelerine bilgilendirme yapıldı mı?

16. Vakanın tekrarlanmaması için alınacak önlemler belirlendi mi?

17. Etkilenen sistemler vaka öncesindeki sağlıklı yapıya döndürüldü mü?

18. Gedik Yatırım Menkul Değerler A.Ş. bilgi sistemleri politikaları / prosedürleri yaşanan zafiyete bağlı olarak vakanın tekrar yaşanmasını engelleyecek şekilde güncellendi mi?

19. Vaka ek bir politika / prosedürle engellenebilir miydi?

20. Vakaya bir politika veya prosedürün izlenmemesi mi sebep oldu?

21. Vakanın en az zararla atlatılması için ortaya konan eylemler yeterli miydi? Sistemlerde herhangi bir iyileştirme yapılabilir mi?

22. Bütün sorumlular sürece zamanında dahil oldu mu?

23. Başka bir vakanın yaşanmasını engellemek için iyileştirme yapıldı mı?

23.1. Sistem güncellemeleri

23.2. Yazılımların güncellemeleri

23.3. Şifrelerin değiştirilmesi

23.4. Anti-virüs yazılımının güncellenmesi

23.5. Vakanın türüne göre alınması gereken diğer önlemler

24. Bu vakadan neler öğrenildi?

25. Kişisel veri, kanuni olmayan yollarla başkaları tarafından elde edildi mi? (Cevabın "Evet" olması durumunda Gedik Yatırım Menkul Değerler A.Ş. bu durumu en kısa sürede kişisel veri sahibi ilgiliye ve Kişisel Verilerin Korunması Kurulu'na bildirir.)

26. (Varsa) Kişisel veri ihlaline yönelik Kişisel Verilerin Korunması Kurulu'na bildirim yapıldı mı?