1. AMAÇ

Bu planın amacı, özel sektör kuruluşu olan Kızılbük Gayrimenkul Yatırım Ortaklığı A.Ş. bünyesinde gerçekleşebilecek siber olaylara (özellikle fidye yazılımları ve phishing/sosyal mühendislik saldırıları) karşı hızlı, koordineli ve etkin müdahale sağlamak; kritik iş süreçlerinin kesintiye uğramasını ve veri kaybını en aza indirmektir.

2. KAPSAM

Bu plan;

- Kızılbük Gayrimenkul Yatırım Ortaklığı A.Ş.'nin sahip olduğu veya sorumluluğundaki tüm bilgi sistemlerini (sunucular, istemciler, ağ cihazları, mobil cihazlar, bulut sistemleri vb.),
- Kurumsal ve kişisel veri içeren tüm uygulamaları (ERP, CRM, e-posta sistemleri vb.),
- Kurum çalışanları, taşeronlar ve iş ortakları tarafından kullanılan bilgi sistemlerini kapsar.

3. TANIMLAR VE KISALTMALAR

- SOME: Siber Olaylara Müdahale Ekibi
- USOM: Ulusal Siber Olaylara Müdahale Merkezi
- SOC: Güvenlik Operasyon Merkezi (varsa, dış hizmet dâhil)
- SIEM: Güvenlik Bilgi ve Olay Yönetimi sistemi
- EDR: Uç Nokta Tespit ve Müdahale
- Olay (Incident): Kurumun bilgi varlıklarının gizlilik, bütünlük veya erişilebilirliğini olumsuz etkileyen ya da etkileme potansiyeli olan her türlü siber güvenlik vakası
- Fidye Yazılımı (Ransomware): Sistem veya dosyaları şifreleyerek erişilemez hâle getiren ve karşılığında ödeme talep eden zararlı yazılım türü
- Phishing (Oltalama): Genellikle e-posta, SMS veya sahte web sitesi üzerinden kullanıcıdan parola, kart bilgisi vb. kritik bilgiler elde etmeye yönelik saldırı türü

4. KURUMSAL ÇERÇEVE VE MEVZUAT

4.1. KVKK ve Kişisel Veri Koruma Yükümlülükleri

Kızılbük Gayrimenkul Yatırım Ortaklığı A.Ş., 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve ilgili ikincil mevzuat kapsamında "veri sorumlusu" sıfatıyla aşağıdaki yükümlülükleri yerine getirir.

- Kişisel verilerin işlenmesi, aktarılması, saklanması ve imhasına ilişkin süreçleri KVKK'ya ve Kurul kararlarına uygun şekilde tasarlar ve yürütür.
- Kişisel verilerin hukuka aykırı olarak işlenmesini, hukuka aykırı erişilmesini ve yetkisiz ifşasını önlemek amacıyla gerekli teknik ve idari tedbirleri alır.
- Gerekli olduğu hallerde VERBIS kaydı, aydınlatma metinleri, açık rıza süreçleri, saklama ve imha politikaları gibi dokümantasyonu oluşturur, güncel tutar.

4.2. KVKK ve Kişisel veri ihlali durumunda bildirim yükümlülükleri:

- Kızılbük Gayrimenkul Yatırım Ortaklılığı A.Ş., kişisel veri ihlalini öğrendiği andan itibaren **mümkün olan en kısa sürede ve en geç 72 saat içinde** Kişisel Verileri Koruma Kurumu'na (KVKK Kurulu) bildirimde bulunur.
- Bildirim; ihlalin niteliğini, etkilenen kişi gruplarını ve veri kategorilerini, ihlalin muhtemel sonuçlarını ve alınan/alınması planlanan önlemleri içerir.
- 72 saat içinde tüm bilgilere ulaşılamaması halinde, eldeki bilgilerle **kısmi bildirim** yapılır; eksik kalan bilgiler tespit edildikçe Kurum'a ayrıca bildirilir.
- İhlalden etkilenen ilgili kişilere, ortaya çıkabilecek zararların azaltılması amacıyla **uygun ve makul süre içinde** ayrıca bilgilendirme yapılır.
- Bu kapsamda SOME/SOC birimi, Bilgi Güvenliği/BT, Hukuk ve Uyum birimleri ile koordineli şekilde çalışarak kişisel veri ihlali tespitini, analizini, iç ve dış bildirimlerini ve düzeltici faaliyetleri işletmekle yükümlüdür.

4.3. Sektöre Özel Düzenleyici Kurumlar (SPK vb.)

Kızılbük Gayrimenkul Yatırım Ortaklığı A.Ş., faaliyet gösterdiği sektör itibarıyla başta **Sermaye Piyasası Kurulu (SPK)** olmak üzere ilgili düzenleyici kurumların yayımladığı düzenlemelere uyar. Sermaye piyasası kurumları için özellikle aşağıdaki düzenlemeler esas alınır.

- **Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10)**
- **Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2)**

Bu çerçevede Kızılbük Gayrimenkul Yatırım Ortaklığı A.Ş.

- Bilgi sistemleri mimarisini, güvenlik kontrollerini, iş sürekliliği ve felaket kurtarma yapısını ilgili SPK düzenlemelerine uyumlu biçimde tasarlar ve işletir.
- Bilgi sistemlerinde meydana gelen, **faaliyetlerin sürekliliğini veya sermaye piyasalarının güven ve istikrarını etkileyebilecek önem ve büyüklükteki** olayları (sistem kesintileri, kritik uygulamaların devre dışı kalması, veri bütünlüğü ihlali, siber saldırılar vb.) belirlenmiş usul ve süreler içinde SPK'ya (Yatırımcı İlişkileri) ve/veya ilgili piyasa işleticilerine bildirir.
- SPK düzenlemeleri ile uyumlu iç politika, prosedür ve kayıt düzenini (log, denetim izi, konfigürasyon kayıtları, değişiklik yönetimi kayıtları vb.) sürdürür.

Kurum (Yatırımcı İlişkileri), ilgili mevzuat kapsamında ortaya çıkabilecek bildirim yükümlülüklerini (kişisel veri ihlali, finansal sistem etkilenmesi vb.) yerine getirmekle yükümlüdür.

5. SOME Organizasyonu

5.1. Roller ve Sorumluluklar

5.1.1. SOME Lideri

- Olay müdahale sürecini başlatır, yönetir ve kapatır.
- Üst yönetime ve gerekiyorsa düzenleyici kurumlara raporlama yapar (SPK'ya Yatırımcı İlişkileri yapar).
- Sistemin devre dışı bırakılması, hizmet kesintisi, müşteri bilgilendirmesi gibi kritik kararları üst yönetim ile birlikte alır.

5.1.2. SOME Teknik Analist(ler)

- SIEM, EDR, antivirüs, IDS/IPS gibi sistemlerden gelen alarmları analiz eder.

- Olayın türünü, kaynağını, kapsamını ve etkisini tespit eder.
- Gerekirse zararlı yazılım analizi, log analizi ve adli bilişim faaliyetlerini yürütür.

5.1.3. Sistem ve Ağ Yöneticileri

- Sunucular, istemciler ve ağ ekipmanları üzerinde izolasyon, müdahale ve kurtarma işlemlerini uygular.
- Yedeklerden geri yükleme ve sistemleri normal duruma döndürme süreçlerinden sorumludur.

5.1.4. Uygulama Sahipleri

- Sorumlu oldukları iş uygulamalarında olayın etkisini değerlendirir.
- Kullanıcıları etki ve planlanan kesintiler konusunda SOME ile koordineli şekilde bilgilendirir.

5.1.5. Hukuk, Yatırımcı İlişkileri ve İnsan Kaynakları

- Olayın hukuki boyutunu değerlendirir (sözleşmeler, SPK, KVKK, iş hukuku vb.).
- Gerekirse çalışanlarla ilgili disiplin süreçlerini yürütür.
- Otorite ve resmi kurumlara yapılacak bildirimlerde SOME'ye destek olur.

5.1.6. Yatırımcı İlişkileri (Yİ), Kurumsal İletişim

- Müşteri, tedarikçi ve kamuoyuna yapılacak açıklamaları hazırlar.
- Tüm açıklamalar Yatırımcı İlişkileri görüşü, SOME Lideri ve üst yönetim onayı ile yapılır.

5.2. SOME İletişim Listesi

- SOME Lideri:
- SOME Teknik Analist:
- Sistem Yöneticisi:
- Ağ Yöneticisi:
- Yatırımcı İlişkileri:
- Hukuk Temsilcisi:
- Kurumsal İletişim:

6. Olay Sınıflandırma ve Önceliklendirme

6.1. Hazırlık

- SOME politika ve prosedürlerinin onaylanması ve personele duyurulması
- İzleme altyapısının kurulması (SIEM, EDR, log yönetimi vb.)
- Kritik sistemler için yedekleme stratejisi ve geri dönüş testleri
- Fidye yazılımı ve phishing özelinde:
- E-posta güvenlik kapıları (spam, phishing filtreleri)
- Makro kısıtlamaları, en az ayrıcalık prensibi
- Kullanıcı farkındalık eğitimleri ve phishing simülasyonları

6.2. Tespit ve Bildirim

- Olaylar aşağıdaki kanallardan tespit edilir:
- SIEM/EDR/Antivirüs/IDS/IPS uyarıları
- Kullanıcı bildirimleri (Help Desk, e-posta, telefon)
- Dış kaynak bildirimleri (iş ortakları, tedarikçiler, USOM vb.)

Tespit edilen her olay için:

1. Olay, SOME olay yönetim sistemine (ticket, takip tablosu vb.) kaydedilir.

2. Kayıtta en az şu alanlar bulunur:

- Olay No, Tarih-Saat
- Bildiren kişi/birim
- Kısa açıklama
- Etkilenen sistem(ler)
- İlk değerlendirme (şüpheli/gerçek olay)

6.3. İlk Değerlendirme ve Sınıflandırma

- SOME Teknik Analist, olayın gerçek bir siber olay olup olmadığını teyit eder.
- Olay türü (fidye yazılımı, phishing, yetkisiz erişim, DDoS, veri sızıntısı vb.) belirlenir.
- Etki ve kapsam analizine göre olay seviyesi atanır.
- Gerekli görülürse SOME Lideri ve ilgili yöneticilere eskalasyon yapılır.

6.4. Müdahale: İzolasyon – Bastırma – Temizleme

Genel adımlar:

1. İzolasyon:

- Etkilenen sistem ağdan ayrılır veya ilgili VLAN/firewall kuralı ile izole edilir.
- Gerekirse kullanıcı hesabı kilitlenir, parolalar sıfırlanır.

2. Bastırma (Containment):

- Saldırganın yatay hareketi (lateral movement) engellenir.
- Geçici ek güvenlik kuralları (IP bloklama, port kapatma, ek izleme) devreye alınır.

3. Temizleme (Eradication):

- Zararlı yazılım ve artefaktları kaldırılır.
- Kullanılan zafiyetler yamalanır veya yapılandırma değişiklikleri yapılır.
- Gerekirse sistem yeniden kurulur.

6.5. Kurtarma (Recovery)

- Sistemler kontrollü şekilde tekrar devreye alınır.
- Gerekirse güvenli yedeklerden geri dönüş yapılır.
- Bir süre boyunca normalden daha sık log/olay izleme yapılır.

İlgili birimler ve kullanıcılar hizmetin normale döndüğü konusunda bilgilendirilir.

6.6. Olayın Kapatılması ve İyileştirme

- Ayrıntılı olay raporu hazırlanır.
- Kök neden analizi yapılır (patch eksikliği, zayıf parola, kullanıcı hatası, yanlış yapılandırma vb.).
- Tekrarını engellemek için ek kontrol, prosedür ve eğitim planlanır.

- Üst yönetime özet yönetim raporu sunulur.

7. Özel Senaryo 1: Fidye Yazılımı (Ransomware) Olay Müdahale Planı

7.1. Senaryo Tanımı

Kurum içindeki bir veya birden çok sistemdeki dosyalar şifrelenmiş, masaüstünde fidye notu bırakılmış ve saldırgan, ödeme karşılığı şifre çözme anahtarı vaat etmektedir.

7.2. Amaç

- Fidye yazılımının kurum içinde yayılımını durdurmak
- Mümkünse veri kaybını yedeklerden gidererek sistemi geri yüklemek
- Müşteri ve kişisel verilerin etkilenip etkilenmediğini değerlendirmek
- İleride benzer saldırıları önlemek

7.3. İlk Tespit ve Acil Aksiyon Checklist'i

- Kullanıcıdan/EDR'den gelen ilk bildirim alınır.
- Fidye notu, şifrelenmiş dosya uzantıları ve ekran görüntüleri kaydedilir.
- Etkilenen cihaz hemen ağdan izole edilir (kablo çıkarma, Wi-Fi kapatma, VLAN izolasyonu vb.).
- Etkilenen cihaz kesinlikle yeniden başlatılmaz veya formatlanmaz (adli analiz için).
- SOME Lideri bilgilendirilir, olay seviyesi belirlenir (genellikle Seviye 1 veya 2).

7.4. Analiz ve Yayılımın Durdurulması

- SIEM/EDR üzerinden aynı zararlı göstergelerini (hash, dosya adı, IP, domain) içeren başka sistemler aranır.
- Etkilenen diğer sistemler de hızlıca izole edilir.
- Domain Controller, dosya sunucuları ve kritik veri tabanı sunucularında şüpheli aktiviteler incelenir.
- Gerekirse tüm kullanıcı parolaları veya belirli grupların parolaları toplu olarak sıfırlanır.

7.5. Fidye Ödemesi Politikası

Kızılbük Gayrimenkul Yatırım Ortaklığı A.Ş., fidye ödemesinin veriyi geri getireceğine dair bir garanti bulunmadığından ve hukuki/etik riskler nedeniyle kural olarak fidye ödemez.

Fidye ödeme kararı istisnai hallerde üst yönetim, hukuk ve SOME Lideri ortak değerlendirmesi ile verilebilir.

7.6. Kurtarma ve İş Sürekliliği

- Güvenli olduğu doğrulanan yedeklerden geri dönüş planı hazırlanır.
- Geri yükleme önce test ortamında denenir (mümkünse).
- Geri yüklenen sistemler açılmadan önce antivirüs/EDR taraması yapılır.

Kritik iş süreçleri için önceliklendirilmiş bir geri dönüş sırası uygulanır (önce muhasebe/finans, ERP, e-posta vb.).

7.7. Raporlama ve İyileştirme

- Olayda kullanılan giriş noktası (phishing mail, zafiyet, zayıf parola vb.) netleştirilir.
- Ağ segmentasyonu, yedekleme yapısı, patch yönetimi ve kullanıcı farkındalık alanlarında eksikler belirlenir.
- Gerekli ek kontroller ve prosedür değişiklikleri planlanır ve uygulanır.

8. Özel Senaryo 2: Phishing (Oltalama) Olay Müdahale Planı

8.1. Senaryo Tanımı

Kurum çalışanlarına sahte e-posta/sms gönderilmiş, kullanıcıdan parola, kart bilgisi veya dosya indirmesi istenmiştir. Bir veya daha fazla çalışan bağlantıya tıklamış ve bilgilerini paylaşmış veya zararlı dosyayı çalıştırmıştır.

8.2. Amaç

- Ele geçirilen kullanıcı hesaplarının hızlıca güvence altına alınması
- Saldırganın kurum sistemlerine erişiminin kesilmesi
- Çalışanları bilgilendirmek ve benzer saldırıların tekrarını önlemek

8.3. İlk Tespit ve Aksiyon Checklist'i

- Phishing e-postası/sms'i SOME'ye iletilir (ekran görüntüsü, tam başlık bilgileri, link).
- E-postanın kimlik bilgileri (gönderen adresi, domain, URL, ekteki dosya hash'i) kaydedilir.
- Aynı phishing e-postasının başka kullanıcılara da ulaşıp ulaşmadığı e-posta geçidi/SIEM üzerinden kontrol edilir.
- Mümkünse e-posta gateway üzerinden toplu silme/karantina işlemi uygulanır.
- Olası tıklayan/kullanıcı bilgisi giren çalışan listesi çıkarılır.

8.4. Etkilenen Hesapların Güvence Altına Alınması

- Kullanıcı hesap parolaları derhal sıfırlanır (e-posta, VPN, domain, SaaS uygulamaları).
- Çok faktörlü kimlik doğrulama (MFA) varsa tekrar kaydedilir/doğrulanır.
- Şüpheli oturumlar sonlandırılır (O365, Google Workspace, VPN, uzak masaüstü vb.).
- Hesap hareket kayıtları (loglar) incelenerek yetkisiz erişim, veri indirme, kural değiştirme vb. aktiviteler aranır.

8.5. Kullanıcı Bilgilendirme ve Farkındalık

- Olayla ilgili kısa ve anlaşılır bilgilendirme e-postası tüm personele gönderilir:
- Saldırının örneği (link/ek gösterilmeden)
- Nelere dikkat edilmesi gerektiği
- Şüpheli e-postaların nereye iletileceği (SOME / Help Desk adresi)
- Olay sonrası hedefli kısa phishing farkındalık eğitimi organize edilir.

8.6. Teknik İyileştirmeler

- E-posta güvenlik politikaları (DMARC, DKIM, SPF, antispam/anti-phishing kuralları) gözden geçirilir.
- URL filtreleme, sandbox, makro kısıtlamaları değerlendirilir.
- "Phishing raporlama butonu" gibi kullanıcıya kolay bildirim yöntemleri devreye alınır (mümkünse).

9. İletişim ve Eskalasyon

9.1. İç İletişim

- Olayla ilgili tüm teknik ve idari iletişim, [örneğin "SOME-Mail-Listesi@[kurum]"] üzerinden yürütülür.
- Acil durumlarda telefon çağrısı/mesajlaşma kullanılabilir; ancak özet bilgi mutlaka resmi kanala kaydedilir.

Örnek Eskalasyon Tablosu:

Seviye 1: SOME Lideri, BT Direktörü, Üst Yönetim ve Yatırımcı İlişkileri (Yİ) – Maks. Bildirim Süresi: 30 dakika

Seviye 2: SOME Lideri, İlgili İş Birimi Yöneticisi – Maks. Bildirim Süresi: 2 saat

Seviye 3: SOME Lideri – Maks. Bildirim Süresi: 4 saat

Seviye 4: SOME Teknik Analist – Maks. Bildirim Süresi: Gün içinde

9.2. Dış İletişim

- Müşteri, tedarikçi ve iş ortaklarına yapılacak bildirimler Yatırımcı İlişkileri, Kurumsal İletişim ve Hukuk birimi koordinasyonunda gerçekleştirilir.
- Resmi kurumlara yapılacak olası bildirimler (kişisel veri ihlali vb.) Yatırımcı İlişkileri, Hukuk ve SOME Lideri koordinasyonunda yapılır.
- Basın açıklamaları sadece yetkilendirilmiş sözcü tarafından yapılır.

10. Kayıt Tutma ve Dokümantasyon

- Her olay için aşağıdaki dokümanlar en az 5 yıl saklanır:
- Olay Kayıt Formu
- Olayla ilgili loglar ve teknik analiz notları
- Yazışmalar, bilgilendirme e-postaları
- Nihai olay raporu ve yönetim özeti

11. Eğitim, Farkındalık ve Tatbikat

- SOME ekibi için yılda en az 1 teknik tatbikat (fidye yazılımı ve phishing senaryolu).
- Tüm çalışanlar için düzenli siber güvenlik farkındalık eğitimleri:
- Phishing örnekleri
- Parola ve MFA kullanımı
- USB/taşınabilir medya riskleri
- Yılda en az bir "masa başı tatbikat" ile bu planın gözden geçirilmesi.

12. Gözden Geçirme ve Güncelleme

- Bu plan en az yılda bir kez SOME Lideri başkanlığında gözden geçirilir.
- Büyük bir siber olay sonrası, önemli mevzuat değişikliklerinde veya organizasyonel değişikliklerde ayrıca revize edilir.
- Planın sürüm numarası ve revizyon tarihi, Word dokümanının ilk sayfasında belirtilir.

EKLER

Ek-1: Olay Kayıt Formu Örneği

Olay Numarası:

Tarih/Saat:

Bildiren Kişi/Birim:

Olay Türü: (Fidye Yazılımı / Phishing / Diğer)

Olay Seviyesi: (1–4)

Etkilenen Sistem/Servisler:

Kısa Olay Tanımı:

Yapılan İlk İşlemler:

İzolasyon ve Müdahale Adımları:

Kurtarma Adımları:

Olayın Kök Nedeni:

Alınan/Kalıcı Önlemler:

Olayı Kapatan SOME Personeli:

Kapanış Tarihi: