BİTBNS KRİPTO VARLIK ALIM SATIM PLATFORMU ANONİM ŞİRKETİ

İŞ SÜREKLİLİĞİ VE KURTARMA PLANI

BİTBNS KRİPTO VARLIK ALIM SATIM PLATFORMU ANONİM ŞİRKETİ

İŞ SÜREKLİLİĞİ VE KURTARMA PLANI

1. AMAÇ VE KAPSAM

İşbu İş Sürekliliği ve Kurtarma Planı ("**Plan**") 6362 sayılı Sermaye Piyasası Kanunu ("**Kanun**") ile III-35/B.1 Kripto Varlık Hizmet Sağlayıcıların Kuruluş ve Faaliyet Esasları Hakkında Tebliğ ("**Faaliyet Esasları Tebliği**") ve III-35/B.2 Kripto Varlık Hizmet Sağlayıcıların Çalışma Usul ve Esasları ile Sermaye Yeterliliği Hakkında Tebliğ ("**Çalışma Usulleri Tebliği**") başta olmak üzere ilgili sermaye piyasası mevzuatı uyarınca Bitbns Kripto Varlık Alım Satım Platformu Anonim Şirketi ("**Platform**") nezdinde gerçekleşecek kripto varlık kaybı sonucu doğurabilecek eylem ve risklerin belirlenmesi, bu risk ve eylemlerin gerçekleşmesi durumunda alınacak aksiyonlara yönelik genel esasları belirlemektedir.

İşbu Plan ile, müşteri hizmetlerinin devamlılığının sağlanması, mevzuata uyum sürecinin yürütülmesi ve müşteri ve Platform varlıklarının korunması amaçlanmaktadır.

İşbu Plan, Faaliyet Esasları Tebliği'nin 47/4'üncü maddesi uyarınca Platform'un internet sitesinde yayımlanır.

2. BEKLENMEDİK DURUM

Beklenmedik Durum, bir Platform'ca sunulan bir hizmetin planlanmamış bir şekilde ve Platform nezdindeki kripto varlıkların kaybı sonucunu doğuracak şekilde kesilmesidir.

Platform, Beklenmedik Durum'a karşı; normal hizmet operasyonlarının mümkün olan en kısa sürede eski haline getirecek ve Beklenmedik Durum'un etkisini minimum seviyeye indirecektir.

2.1. Beklenmedik Durum Önem Seviyeleri

Beklenmedik Durum önem seviyesi meydana geldiği yer, meydana geldiği zaman ve kripto varlıklara vereceği potansiyel zararlar düşünülerek her olay için ayrı ayrı belirlenir.

3. BEKLENMEDİK DURUM'DA ALINACAK TEDBİRLER:

Platform, Beklenmedik Durum'un gerçekleşmesi halinde, Beklenmedik Durum'un niteliğine göre aşağıdaki tedbirleri alır:

- Sıcak cüzdanlarda bulunan kripto varlıkların güvenli yöntemler kullanarak ivedi şekilde soğuk cüzdanlara çekilmesi,
- Tehdit altındaki veya Beklenmedik Durum sebebiyle etkilenen sistem veya cüzdanların diğer sistem ve cüzdanlardan izole edilmesi,
- Karşılaşılan durumun, etkilenen sistem, cüzdan ve olay sebebiyle oluşabilecek sistemsel zayıflık ve arızaların değerlendirilmesi,
- Mevzuat uyarınca tutulması gereken tüm belge ve kayıtların tutulmaya devam edilmesinin sağlanması,
- Tehdidin ortadan nasıl kaldırılabileceği ve sistem ile cüzdan güvenliğinin tekrar nasıl sağlanacağı süreçlerini,
- Tehdidin veya olaya sebep olan zayıflığın kaynağının tespit edilmesi halinde kullanılabilecek araç veya yöntemlerin belirlenmesi,

- Platform'un faaliyete devam etmeme yönünde karar alması halinde müşterilere ait kripto varlıkların transfer sürecinin belirlenmesi,
- Kurul'un alınan tedbirler hakkında bilgilendirilmesi.

3.1. Kripto Varlıkların Soğuk Cüzdanlara Aktarılması

Sıcak cüzdanlarda meydana gelebilecek arıza, siber saldırı, sistemsel zayıflık veya operasyonel hata gibi durumların kripto varlık kaybı riskini artırabileceği dikkate alınarak; sıcak cüzdanlarda tutulan kripto varlıklar, güvenli transfer yöntemleri ve çoklu imza mekanizmaları kullanılarak en kısa sürede soğuk cüzdanlara aktarılır.

Transfer işlemleri, bütünlük ve izlenebilirlik esaslarına uygun olarak gerçekleştirilir.

3.2. Etkilenen Sistem veya Cüzdanın İzolasyonu

Tehdit altında olduğu tespit edilen veya Beklenmedik Durum'un gerçekleşmesi (siber saldırı, sistem arızası, güvenlik ihlali vb.) nedeniyle etkilenen sistemlerin veya cüzdanların, olayın yayılımını önlemek ve diğer varlıkların güvenliğini sağlamak amacıyla, derhal diğer sistemlerden ve cüzdanlardan izole edilmesi.

İzolasyon işlemleri kontrollü, kayıtlı ve doğrulanabilir yöntemlerle gerçekleştirilir.

3.2.1. Cüzdan İzolasyonu

Tehdit altında olduğu tespit edilen ya da Beklenmedik Durum'un gerçekleştiği cüzdanlara yönelik, içerdikleri kripto varlıkların güvenliğinin sağlanması esastır.

Olası bulaşıcı etkileri ve zincirleme kayıpları önlemek amacıyla, acil şekilde Platform'un diğer cüzdanlarından ve işlem ağlarından fiziksel veya mantıksal yollarla ayrılır. İzolasyon, cüzdandan varlık çıkışı, yeni giriş veya işlem yapılmasının engellenmesini ve yalnızca yetkili güvenlik prosedürleri çerçevesinde erişim sağlanması gibi tedbirleri içerir.

3.2.2. Sistem İzolasyonu

Tehdit altında olduğu tespit edilen ya da Beklenmedik Durum'un gerçekleştiği sistemlerde zayıflık tespit edilmesi halinde, etkilenen sistem veya bileşenlerin (sunucular, ağ bağlantıları, API'ler ve benzeri) Platform'a ait diğer operasyonel sistemlerden ayrılarak bağımsız çalışma moduna geçirilmesi sağlanır.

Sistem izolasyonu; veri trafiğinin kesilmesi, API erişimlerinin kapatılması, müşteri işlemlerinin askıya alınması ve güvenli kurtarma ortamlarına yönlendirme tedbirlerini içerir.

3.3. Beklenmedik Durum'un İş Akışına Etkisi

Beklenmedik Durum'un ardından, olayın etkilediği sistemler ve cüzdanlar üzerinde oluşabilecek sistemsel zayıflıkların ve arızaların tespit edilerek değerlendirilmesi esastır.

Yapılacak olan değerlendirmede aşağıdaki hususlar göz önünde bulundurulur:

- Etkilenen sistemler ve cüzdanlar üzerinde detaylı bir güvenlik ve bütünlük analizi yapılması,
- Olay sebebiyle oluşan sistemsel zayıflıkların, arızaların ve güvenlik açıklarının kapsamının belirlenmesi,

- Zayıflıkların ve arızaların potansiyel etkilerinin (müşteri varlıkları, veri bütünlüğü, operasyonel süreçler üzerindeki etkiler dahil olmak üzere) analiz edilmesi,
- Tespit edilen zayıflıkların giderilmesine ve güvenlik önlemlerinin güçlendirilmesine yönelik aksiyon planlarının oluşturulması,
- Değerlendirme sonuçlarının kayıt altına alınması ve ilgili birimlerle paylaşılması.

3.4. Belge ve Kayıtların Tutulmaya Devam Etmesi

Beklenmedik Durum ve etkilenen sistemler veya cüzdanlarla ilgili karşılaşılan olayda, mevzuat uyarınca tutulması gereken tüm belge ve kayıtların kesintisiz olarak tutulmaya devam edilmesi esastır.

Bu belgeler, işlem kayıtları, güvenlik raporları, erişim logları gibi ilgili tüm verileri kapsar ve güvenli bir ortamda depolanarak, yalnızca yetkilendirilmiş kişilerin erişimine sunulur. Kayıtların doğruluğu, bütünlüğü ve mevzuata uygunluğu sürekli denetlenir ve gerektiğinde düzenleyici kurumlarla paylaşılmak üzere hazır bulundurulur.

3.5. Tehdidin Kaldırılması

Tespit edilen tehdidin ya da Beklenmedik Durum'un ortadan kalkması halinde Platform'un operasyonel süreçlerinin olağan şekilde gerçekleştirilmesi esastır. Bu amaçla, etkilenen sistem ve cüzdanların güvenliğinin yeniden sağlanması için küresel piyasa standartlarda tedbirler alınacaktır.

Tehdidin kaldırılması süreci, Tespit edilen tehdit ya da Beklenmedik Durum'un hangi sistemde meydana geldiğinin tespit edilmesiyle başlar ve sorunun tüm sonuçlarıyla beraber çözülmesiyle sona erer.

3.5.1. Durumun Gerçekleşmesi ve Haberleşme

Kripto varlık kaybıyla sonuçlanabilecek Beklenmedik Durum'lar ve tehditleri tam ya da yarı otomasyon sistemleri veya manuel olarak tespit edilir.

Tespit edilen tehdidin hangi sistemde tespit edildiğini de içerir ileti, Platform'un ilgili tüm birimlerine gönderilir.

3.5.2. Etkilerinin Azaltılması

Tespit edilen tehdit giderilmeden önce, tehdidin potansiyel sonuçları da göz önünde bulundurularak etkilerinin azaltılması için gerekli analizler yapılır ve önlemler alınır. Bu aşamada sorun raporlanırken, operasyonel departmanlar ve müşteriler de bilgilendirilir.

Analiz ve değerlendirmeler yapılırken, sistem bağlantıları, sistem izlemesi günlükler ve kodlar başta olmak üzere detaylı bir inceleme gerçekleştirilir. Gerçekleştirilen analizler ve değerlendirmeler kaydedilir.

3.5.3. Tehdit Analizi

Tehdidin potansiyel etkilerine yönelik yapılan ön değerlendirmeyi müteakiben yapılan etki azaltılmasının ardından, tehdit tüm yönleriyle ele alınarak asıl değerlendirme yapılır. Asıl değerlendirmede, ilgili tüm paydaşlar acil durum müdahalesi için azami çaba gösterirler.

3.5.4. Tehdidin Çözümü

Tehdidin detaylıca değerlendirilmesinin ardından, tehdidin bertaraf edilebilmesi için en etkili çözüm seçilir. İşbu seçimde müşteri ile Platform kripto varlıklarının kaybedilmesi tehlikesi göz önünde bulundurulur.

Beklenmedik Durum'un ortadan kalkmasının ardından, Platform tarafından derhal kök neden analizi yapılır.

3.5.5. Sistem ve Cüzdan Güvenliğinin Yeniden Tesisi

Tehdit ortadan kaldırıldığında, etkilenen sistemler ve cüzdanların güvenliği yeniden sağlanır. Bu süreç, tehdit kaynağının tamamen ortadan kaldırılması, güvenlik açıklarının kapatılması ve sistemlerin sağlam bir şekilde yeniden yapılandırılmasını içerir.

Sistemin ve cüzdanın güvenliğinin yeniden sağlanabilmesi için, ilk olarak tehdit kaynağının tespit edilip izole edilmesi, ardından tüm güvenlik önlemlerinin gözden geçirilmesi ve güçlendirilmesi sağlanır. Sistem üzerinde yapılan iyileştirmeler ve güvenlik testlerinin başarıyla tamamlanmasının ardından, güvenliğin yeniden tesis edildiği onaylanır ve normal operasyonel sürece dönülür.

3.6. Tehdidin Kök Kaynağının Tespitinde Yöntem

Beklenmedik Durum'un ardından tehdidin veya olaya sebep olan zayıflığın kaynağının tespit edilmesi amacıyla uygun araçlar ve yöntemler kullanılır. Bu kapsamda, sistem loglarının analizi, ağ trafiği izleme araçları, güvenlik olay yönetim sistemleri (*SIEM*), adli bilişim analizleri ve saldırı tespit sistemleri gibi teknikler kullanılarak olayın çıkış noktası ve yayılma şekli belirlenir.

Yapılan tüm tespit çalışmaları kayıt altına alınır ve ilgili birimlerle paylaşılır.

3.7. Platform'un Faaliyetine Son Vermesi Halinde

Platform tarafından faaliyete devam edilemeyeceği yönünde karar verilmesi halinde, müşterilere ait kripto varlıkların güvenli, şeffaf ve hızlı bir şekilde transfer edilmesi esastır.

Bu süreçte, müşterilere ait tüm kripto varlıklar önceden belirlenmiş güvenli transfer prosedürleri çerçevesinde, müşterilerin talep edeceği cüzdan adreslerine transfer edilir.

Transferler, müşteri kimlik doğrulamasının yapılması, transfer işlemlerinin kayıt altına alınması ve her adımın şeffaf bir şekilde raporlanması suretiyle gerçekleştirilir. Kripto varlık transferleri sırasında, varlık güvenliğini ve bütünlüğünü sağlamak için çoklu imza mekanizmaları, transfer limiti kontrolleri ve manuel onay süreçleri uygulanır.

Tüm transfer işlemleri tamamlanıncaya kadar denetim mekanizmaları devrede tutulur ve işlemlerin sonuçları düzenli olarak tutulur.

3.8. Kurul'un Bilgilendirilmesi

Beklenmedik Durum'un gerçekleşmesi veya bir tehdidin ortaya çıkması halinde alınan önlemler, yapılan müdahaleler ve gerçekleştirilen kurtarma adımları hakkında, mümkün olan en kısa sürede Kurul'a resmi bildirimde bulunulması esastır.

Bildirim; Beklenmedik Durum'un veya tehdidin kapsamı, etkilediği sistem veya cüzdanlar, alınan güvenlik ve kurtarma önlemleri ile mevcut durum değerlendirmesini içerecek şekilde hazırlanır. Kurul'a

iletilen bilgiler güncel, doğru ve doğrulanabilir nitelikte olur. Olayın gelişimine göre ilave bilgilendirmeler yapılır ve talep edilmesi halinde Kurul'a ayrıntılı rapor sunulur.

4. KURTARMA PLANININ UYGULANMASI

İşbu Plan'ın uygulamaya konması durumunda Platform risk yönetim birimi tarafından Plan'ın iş akış prosedürlerine uygun olarak yürütülüp yürütülmediğine ve karşılaşılan durumun müşteri varlıklarına ve Platform'a olası mali etkisine ilişkin bir değerlendirme raporu hazırlanır ve Platform yönetim kuruluna sunulur. Ayrıca söz konusu raporun bir örneği Kurul'a iletilir.

İşbu Plan'ın uygulamaya konmasından sonraki on beş (15) gün içinde Platform tarafından rezerv kanıt denetimi yaptırılır.

4.1. Veri Tabanının Oluşturulması

Her Tehdit veya Beklenmedik Durum'lar; ileride başvurmak ve öğrenmek için temel veriler olarak bilgi tabanında arşivlenecektir. Böylece Platform personelleri ve birimleri arasında bilgi paylaşımını kolaylaştırılacaktır.

Platform, Tehdit ve Beklenmedik Durum'lara karşı geliştireceği çözüm mekanizmalarında gerçek zamanlı arşivlerden faydalanacak ve en uygun kişilerin tehdit ve beklenmedik durumunun tespiti anından itibaren sürece dahil edilmesini sağlayacaktır.

5. SON HÜKÜMLER

5.1. Kurtarma Planı Sorumluları

İşbu Plan ve buna ilişkin iş akış prosedürlerinden sorumlu olmak üzere biri en az genel müdür yardımcısı düzeyinde olmak üzere iki personelin yönetim kurulu tarafından atanması gerekir. Yönetim kurulu tarafından atanan iki personele ilişkin elektronik posta adresi, telefon ve faks numaraları dahil olmak üzere her türlü iletişim bilgisi Kurul'a ve Kurul'ca belirlenecek diğer kuruluşlara bildirilecektir.

5.2. Gözden Geçirme

İşbu Plan, Kurul tarafından yapılan mevzuat değişikliklerinin işlenmesi ve uygulamada kazanılan deneyimler dikkate alınarak gözden geçirilir ve Plan'da gerekli güncellemeler yapılır.

5.3. Müşterilere Bildirim

İşbu Plan'da yapılacak değişiklikler müşterilere bildirilir. Bildirimin yapıldığına ilişkin ispat yükü Platform'a aittir. Bu noktada gerekli kayıtlar Platform tarafından oluşturulacaktır.