KARAPARANIN AKLANMASININ ÖNLENMESİ: TEMEL KONULAR

Örnek Olay 7: Sanal Varlıklar

"Sanal Varlıklar", Dağıtılmış Defter Teknolojisi (Distributed Ledger Technology-DLT) tarafından desteklenen geniş ve yeni bir varlık sınıfını ifade eder. DLT, verilerin paylaşılan bir ağ üzerinde birden fazla yerde ("merkezi olmayan") depolanmasına olanak tanır ve katılımcıların Bitcoin gibi sanal varlıkların alınması ve aktarımı gibi faaliyetlerde kullanımına olanak tanır. Sanal varlıklar, geleneksel varlıklara ve ödemelere kıyasla benzersiz özellikler, avantajlar ve dezavantajlar sunar. Genellikle düzenlenmiş finansal sistemin dışında değer elde etmek, taşımak, depolamak ve fonların kaynağını veya hedefini gizlemek amacıyla; karapara aklayıcılar ve terörist finansörler tarafından bu benzersiz özelliklerin nasıl kullanılabileceği konusunda muhasebe meslek mensupları mutlaka bilgi sahibi olmalıdır.

Sanal varlıklar nasıl kötüye kullanılabilir?

Aşağıdakiler dahil olmak üzere kara para aklamanın herhangi bir aşamasında sanal varlıklar yer alabilir:

- **Öncül suç:** Sanal varlıklar karşılığında yasa dışı mal veya hizmet satarak yasa dışı faaliyetler yoluyla para kazanmak.
- **Yerleştirme:** Haksız elde edilmiş sanal varlıkları geleneksel bir finansal sistem içinde yasal para birimlerine dönüştürmek.
- **Gizleme:** Kripto tabanlı işlemler genellikle blok zinciri analitiği ile takip edilebilir, ancak yasal çerçevenin dışında gerçekleştirildiğinde bir işlem ile herhangi bir kişi arasında herhangi bir bağlantı olmayabilir. Suçlular, kripto işlemleri arasındaki bağlantıları koparmak amacıyla kişisel verilerin anonimleştirilmesi hizmetlerini (tumbler veya mixer gibi) de kullanabilir.
- **Kat kat işlem yapmak:** Yasal varlıkları sanal varlıklara dönüştürmek, sanal varlıkları değiştirmek, sanal varlıkları kendi aralarında dönüştürmek ve sanal varlıkları yasal para birimlerine dönüştürmek.
- **Entegrasyon:** Karaparanın aklanmasına benzer şekilde, geliri meşrulaştırmak ve kirli kriptoyu temizlemek amacıyla kripto ödemelerini kabul eden sanal bir şirket oluşturmak.

Tanımlar

Sanal Varlıklar: Sanal varlık, transfer edilebilen veya ödeme için kullanılabilen değerin dijital bir temsilidir. Yasal dijital para birimlerini içermez.

Kripto Para: Elektronik olarak bir takas aracı olarak kullanılabilen, aktarılan, depolanan ve alınıp satılan kriptografi ile korunan, merkezi olmayan bir sanal varlık. Binlerce kripto paranın en popüleri Bitcoin ve Ether'dir.

NFT (Non-Fungible Token): Tamamen benzersiz bir sanal varlık. Birçok Bitcoin varken, her bir NFT'den yalnızca bir tane vardır. Bunlar genellikle belirli bir sanal sanat eserini veya başka bir sanal veya gerçek mülkü temsil eder.

Sanal Varlık Hizmet Sağlayıcısı (VASP): Aşağıdaki hizmetlerden herhangi birini sağlayan bir işletme:

- Sanal varlıklar ve yasal para birimleri arasında ya da farklı sanal varlıklar arasında transfer veya takas,
- Sanal varlıkların korunması/yönetimi,
- Sanal varlık ihracı ile ilgili finansal hizmetler.

Sanal para cüzdanı: Sanal varlıkları tutmak, depolamak ve aktarmak için kullanılan bir araç.

ÖRNEK OLAY

Colonial Pipeline Fidye Yazılım Saldırısı

Sanal varlıklar, muhasebe meslek mensupları, özellikle denetçiler ve müşterileri tarafından giderek daha fazla görülen siber "fidye yazılımı" saldırıları için hızlı bir ödeme yöntemi haline gelmiştir.

Amerika Birleşik Devletleri'ndeki Colonial Pipeline saldırısı, şirketlerin düzenli olarak uğradığı fidye yazılımı saldırılarının en iyi örneklerindendir. Mayıs 2021'de Colonial Pipeline Şirketinin, beş günlük bir faaliyet durdurması ile sonuçlanan büyük bir fidye yazılımı siber saldırısına uğramıştır. Hackerlar Colonial Pipeline Şirketin'den 4,4 milyon ABD dolarına eşdeğer 75 Bitcoin fidye talep etmiştir. Yetkililer verilen paranın çoğunu geri alabilse de, yapılan araştırmalar, hackerların önceki yıl 47 farklı kaynaktan 90 milyon doların üzerinde Bitcoin aldığını ortaya koymuştur.

Sonuç olarak, bu tür yasadışı gelirlerin, yasal mali sisteme entegre edilmesi gerekecektir. Bu işlemler, muhasebe meslek mensupları tarafından yapılmaktadır. Böyle bir durumda, muhasebe meslek mensupları bu suçları tanımlayarak rapor etme fırsatına sahiptir. Aynı zamanda, fidye yazılımı saldırıları, etkili siber güvenlik kontrollerinin önemini de vurgulamaktadır.

EK YARDIM

Genel rehberlik için FATF'lere bakınız. *Risk Temelli Yaklaşım rehberi meslek mensupları için*. Geçerli düzenleyici gereksinimler dahil ayrıntılı yerel bilgiler için Muhasebe Meslek Örgütünüzle iletişime geçiniz.

⚠ Kilit İşaretler

Karaparanın aklamasının önlenmesine yönelik dikkat edilmesi gereken tüm "geleneksel" konular, sanal varlıklar için de geçerlidir. Bunlara ek olarak aşağıdakilere de dikkat edilmesi gerekmektedir:

- Müşterinin, servetinin büyük kısmını, herhangi bir dijital ayak izi olmaksızın sanal varlıklara yaptığı yatırımlardan elde etmesi.
- Karaparanın aklanmasının önlenmesi ile mücadele ve bu konuda kontrollerin bulunmadığı Sanal Varlık Hizmet Sağlayıcılarından temin edilen sanal varlıkların orantısız bir şekilde, müşterinin servet kaynağını oluşturması.
- Müşterinin, karaparanın aklanmasının önlenmesi ile mücadele ve bu konuda kontrollerin bulunmadığı yüksek riskli bir ülkede sanal varlık değişimi kullanması.
- Müşterinin e-posta ve IP adresleri dahil olmak üzere kimlik bilgilerini sık sık değiştirmesi.

Son zamanlarda gerçekleşen kripto para üzerinden karapara aklama faaliyetleri şu yollarla yapılmıştır:

- Düzenlenmemiş kripto para borsaları (Karapara Aklama Karşıtı/KYC (Know Your Customer) uyumlu).
- Bahis ve oyun siteleri.
- Karıştırma-anonimleştirme hizmetleri (ör. Anonymix).
- Risk yönetimi zayıf olan kripto ATM'leri.
- Ön ödemeli kripto banka kartları.

Muhasebe meslek mensupları, bu tür ürün/hizmetlerden yararlanan önemli faaliyetleri ikinci bir incelemeye, hatta birçok kez incelemeye sevk edilmelidir.

Ne Zaman Geri Çekilmelisiniz?

- Talep edilen hizmetler, yetkinlik alanınız dışında, özel nitelikte ise.
- Fonların kaynağını detaylandıran ticaret veya yatırım kayıtları yoksa.
- Sanal varlığın itibarı, ihraççıları ve borsaları hakkında endişeleriniz varsa.
- Karaparanın aklanmasının önlenmesi ile mücadele ve bu konudaki kontroller ihraççı(lar) ve borsa(lar) tarafından etkin olarak uygulanmıyorsa.
- Müşteri tarafından sağlanan bilgilerin doğruluğu hakkında veya müşteri hakkında endişeleriniz varsa.

Şüpheli İşlem Bildirim Raporu Hazırlama

Varlık transfer işlemlerinde suç faaliyeti veya suç geliri olabileceğinden şüphelenmeniz durumunda, şüphelerinizi yerel Mali İstihbarat Birimi'ne bildirmek isteyebilirsiniz. Bazı ülkelerde bu, muhasebe meslek mensupları için yasal bir zorunluluktur.

TÜRMOB YAYINLAMA İZNİ

Uluslararası Muhasebeciler Federasyonu (IFAC) tarafından Şubat 2022 tarihinde İngilizce olarak yayınlanan, "Anti-Money Laundering: The Basics Installment 7: Virtual Assets", IFAC'tan izin alınarak Ağustos 2022 tarihinde TÜRMOB tarafından Türkçe'ye çevrilmiştir. IFAC yayınlarının tamamı İngilizce olarak yayınlanır. IFAC söz konusu çevirinin doğruluğu ve tamlığı ya da bunların bir sonucu olarak ortaya çıkabilecek eylemler konusunda herhangi bir sorumluluk üstlenmez.

Orijinal Adı: Anti-Money Laundering: The Basics Installment 7: Virtual Assets © Şubat 2022.

Yayın yılı: 2022