Kullanılan İşlem Platformunun ve Bilgisayar Ağının Özellikleri, Riskleri ve Güvenlik Tedbirleri ile Platformda Meydana Gelebilecek Risklere Karşı Kullanılabilecek Alternatif İletişim Yöntemleri

Kullanılan Bilgisayar Ağı ve Şifreleme Sisteminin Olası Riskleri ve Güvenliği SSL Sertifika Güvenliği: Müşterilerimizin online işlemlerini yaptığı platformda 2048 Bit Global Sign SSL sertifikası ile şifrelenerek yüksek düzeyde Organization SSL sertifikası ile güvenlik hizmeti verilmektedir. Bu dijital sertifika, Kurumsal Kimlik Doğrulama ve mümkün olan en yüksek SSL güvenliğini sağlar. Müşterilerimiz bu sertifika ile kurumsal kimliğimizin doğrulandığını, şirketimizin varlığının kanıtlandığını ve online giriş sayfasının Papara Menkul Değerler A.Ş adına ait olduğu nu görür. Bu sayede müşterilerimiz kişisel bilgilerini sadece Papara Menkul Değerler A.Ş ile paylaştıklarından emin olurlar. SSL güvenliği aynı zamanda müşterilerimizin, tüm online işlemlerinin şifrelenip güvenliğinin sağlanması işlevini de yerine getirir.

Sanal Klavye Güvenliği: Online giriş bölümünün kullanımı esnasında kişisel bilgisayarların klavyesine yönelik “Key Logger” isimli çeşitli kötü amaçlı yazılımlara ait riskler bulunmaktadır. Bu tür kötü amaçlı yazılımlar müşterilerin kendi klavyelerinde yazdığı kişisel şifreleri hafızasında tutarak şifre güvenliğini ortadan kaldırmaktadır. Bu nedenle, Papara Menkul Değerler A.Ş şifre girişlerini üst düzeyde güvenlik altına almak amacıyla “Sanal Klavye” uygulamasını tercih olarak müşterilerine sunmaktadır.

Şifre Güvenliği: Müşterilerimiz tarafından kullanılan online işlem merkezinde, iki aşamalı şifre güvenliği uygulanmaktadır. Müşteri kendi tercihi ile giriş ve onay şifrelerini farklılaştırarak dilediği zaman değiştirebilir. Aynı zamanda müşterilerimize elektronik ortamda şifre tahsisi söz konusu olmadığı gibi, şifre değişikliği ve bloke durumunda, müşteriye yetkili kullanıcı tarafından tahsis edilen geçici şifrenin ilk kullanımda değiştirilmesi zorunludur. Şifre değişiklikleri dahil tüm şifre tahsislerinde, müşteri şifresini yetkili personel dahil hiç kimse görememektedir.

Elektronik ortamda emir iletiminde kullanılan işlem platformları; online işlem merkezi, BIST pay senedi ve VIOP işlemleri için veri yayın ekranları ile mobil uygulamalardır.

Emir iletiminin kesintiye uğraması durumunda alternatif işlem yöntemleri, merkez ve merkez dışı örgütlerin aranarak telefonla emir iletilmesi veya veri yayın ekranlarından emir iletimidir.

Veri yayın ekranlarında ise müşterilerin emir ve hesap işlemlerinin tamamı, müşteri bilgisayarı ile kurumumuzun sunucu sistemleri arasında gerçekleşmektedir. Müşterinin işlem bilgileri veri yayın kuruluşu sunucu sistemleri aracılığıyla değil, doğrudan iletilmektedir. Bir kullanıcının işlem yapma yetkisi, izinleri ve limitleri daima kurumumuzun sunucularında tanımlanmaktadır. Tüm işlemlerde istek sunucuya iletilmeden önce müşteri onayı alınmaktadır. Müşterilerimiz tercihe göre, onay aşamasını işlem platformu ayarlarından kapatabilmektedir. Bu işlemlerin tamamında “varsayılan” olarak müşteri onayı zorunlu tutulmaktadır.

Sunucu yazılımları ve web servisleri ile yapılan haberleşmede SSL sertifikası kullanılmaktadır. Şifre bilgileri, cihazın saklama alanlarında (hard disk – SD bellek vb.) saklanmamaktadır. Müşteri cihazları ile sunucu arasında yapılan haberleşmede, şifre bilgisi MD% algoritmasından geçirildikten sonra iletilmektedir. Memory Dump vb. yöntemlerle şifreyi geri oluşturmak mümkün değildir. Müşterilerin yaptığı işlemlere ait log kayıtları, farklı seviyelerde saklanmaktadır. Kullanıcı bilgisayarında saklanan log dosyalarının kapsamını sınırlandırabilmektedir. Sisteme girilen emirlerin log kayıtları, ayrı bir şifreli formatta saklanmaktadır. İşlem terminallerine ilişkin programların kılavuzları yayınlanmakta, müşteri eğitimleri doğrudan yetkili personel tarafından verilmektedir.