Ödeme ve Bilgi Güvenliği Terimleri Sözlüğü

KÜÇÜK ÖLÇEKLİ ÜYE İŞYERLERİ İÇİN VERİ GÜVENLİĞİNİN TEMELLERİ
ÖDEME KARTLARI ENDÜSTRİSİ KÜÇÜK ÖLÇEKLİ ÜYE İŞYERİ GÖREV GÜCÜNÜN BİR ÜRÜNÜ

SÜRÜM 2.0 | AĞUSTOS 2018

PCI Security Standards Council®

Giriş

Bu Ödeme ve Bilgi Güvenliği Terimleri Sözlüğü, Küçük Ölçekli Üye İşyerleri için Veri Güvenliğinin Esaslarının bir parçası olan *Güvenli Ödeme Kılavuzuna ektir*. Bu sözlükle, Ödeme Kartları Endüstrisi (PCI) ve bilgi güvenliği terimlerinin, kolayca anlaşılır bir dilde açıklanması hedeflenmiştir.

Yıldız işaretli (*) terimlerin tanımları, *Ödeme Kartları Endüstrisi (PCI) Veri Güvenliği Standardı (DSS) ve Ödeme Uygulaması ve Güvenliği Standardı (PA-DSS: Terimler ve Tanımlar Sözlüğüne dayanarak ya da bunlardan türetilerek oluşturulmuştur.* Bu sözlüğün son sürümü güvenilir kaynak olarak görülür vengeçerli ve eksiksiz PCI DSS ve PA-DSS tanımları için başvurulmalıdır.

Lütfen aşağıdaki adreslerden Küçük Ölçekli Üye İşyerleri için Veri Güvenliğinin Esaslarını inceleyin:

KAYNAK	URL
Güvenli Ödeme Kılavuzu	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf*
Genel Ödeme Sistemleri	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf*
Ödeme Kuruluşlarınıza Sormanız Gereken Sorular	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf*
Değerlendirme Aracı	*http://www.pcisecuritystandards.org/merchants/ds.org/merchants/* Bu araç yalnızca üye işyerinin bilgi alması amacıyla sağlanmıştır. Üye işyerlerinin bir seçeneği, bu aracı ilgili ödeme alma şekillerine ilişkin güvenli uygulamalar hakkında bilgi edinmek, ilk yanıtlarını vermek ve sonuçlarını görmek için kullanmaktır.

Sözlük

TERİM	TANIM
Adli Bilişim Müfettişi	PCI Adli Bilişim Müfettişleri (PFI'ler), bir kart verisi ihlalinin ne zaman ve nasıl meydana geldiğini belirlemek amacıyla PCI Konseyi tarafından onaylanan şirketlerdir. Finans sektöründe kanıtlanmış araştırma metodolojileri ve araçları kullanarak araştırmalar yaparlar. Ayrıca, sonuçta ortaya çıkan herhangi bir cezai soruşturmada paydaşları desteklemek amacıyla kolluk kuvvetleri ile birlikte çalışırlar.
Ağ *	Fiziksel veya kablosuz araçlarla bağlanan iki veya daha fazla bilgisayar.
Anti-Virüs Yazılımı *	Virüs, solucan, Truva atı, casus yazılım, reklam yazılımı ve korsanlık amaçlı program da dahil olmak üzere kötü niyetli yazılımları ("kötü amaçlı yazılım" olarak da adlandırılır) algılayan, kaldıran ve bunlara karşı koruyan yazılım programı. Ayrıca "kötü amaçlı yazılıma karşı yazılım" olarak da adlandırılır.
Ayrıcalığın Kötüye Kullanımı	Bilgisayar sistemi erişim ayrıcalıklarının kötüte kullanımı. Bunun örnekleri arasında, sistem yöneticisinin kart verilerine kötü amaçla erişimi ya da bir kişinin, bir yöneticinin yükseltilmiş erişim ayrıcalıklarını kötü amaçlı olarak çalıp kullanması sayılabilir.
Bağımsız Terminal	Üye işyerinin sistemi içerisindeki başka herhangi bir cihaza bağlanmaya güvenmeyen ve başka hiçbir işlev yerine getirmeyen bir ödeme terminali. Çalışması için tek gereksinim, İnternet bağlantısı ya da telefon hattıyla işleyiciye bağlı olmasıdır. Terminalin bilgisayarlı elektronik yazarkasa bağlantısı gerektirmesi ya da çok işlevli (mobil cihaz gibi) olması halinde bu terminal, bağımsız bir terminal olmaz.
Banka Kimlik Numarası (BIN)	Bir ödeme kartı numarasının, ödeme kartını kart sahibine veren finans kuruluşunu tanımlayan ilk altı hanesi (veya daha fazla).
Bilgisayar Korsanı	Kontrol ve erişim elde etmek amacıyla bilgisayar sistemlerinin güvenlik önlemlerini atlatmaya çalışan bir kişi veya kuruluş. Genellikle kart verilerini çalmak için bu eylemi gerçekleştirirler.
Çip	"EMV Çip" olarak da bilinir. EMV işlemlerinde, uluslararası şartnamelere uygun olarak işlem yaparken kullanılan bir ödeme kartındaki mikroişlemci (veya "çip").
Çip ve İmza	Tüketicinin mal veya hizmet aldığında EMV Çip özellikli bir ödeme terminaline imzasını kullandığı bir doğrulama işlemi.
Çip ve PIN	Tüketicinin mal veya hizmet aldığında EMV Çip özellikli bir ödeme terminaline PIN kodunu girdiği bir doğrulama işlemi.
Çok Faktörlü Kimlik Doğrulama *	Bir kullanıcının kimliğini doğrulamak için iki veya daha fazla faktör doğrulaması gereken yöntem. Bu faktörler arasında, kullanıcının sahip olduğu bir şey (akıllı kart veya dongle gibi), kullanıcının bildiği bir şey (parola, anahtar parolası veya PIN gibi) ya da kullanıcının olduğu veya yaptığı bir şey (parmak izleri, diğer biyometrik biçimler vb.) olabilir.
Elektronik Yazarkasa (ECR)	İşlemleri kaydedip hesaplayan ve makbuz yazdırabilen, ancak müşteri kartı ödemeleri kabul etmeyen bir cihaz. "Kasa" olarak da adlandırılır.
Entegre Edici/Satıcı	Entegre edici/satıcı, üye işyerlerinin ödeme sistemlerini kurmalarına yardımcı olmaları için birlikte çalıştıkları şirketlerdir. Bu yardım, kurulum, yapılandırma ve destek içerebilir. Bu şirketler, hizmetlerinin bir parçası olarak ödeme cihazları veya uygulamaları da satabilir. Ayrıca bkz. *Nitelikli Entegre Edici Satıcı (QIR)*.
Entegre Ödeme Terminali	Ödeme alan, işlemleri kaydedip hesaplayan ve makbuzları yazdıran bir cihazdaki bir ödeme terminali ve elektronik yazarkasa.
Güçlü Kimlik Doğrulama *	Koruduğu sistemin güvenliğini sağlamak amacıyla bir kullanıcının veya cihazın kimliğini doğrulamak için kullanılır. Güçlü kimlik doğrulama terimi genellikle çok faktörlü kimlik doğrulaması (MFA) anlamına gelir.

Sözlük

TERİM	TANIM
Günlük *	Bilgisayar sistemi veya ağ içinde önceden tanımlanmış bazı olaylar (genellikle güvenlikle ilgili) meydana geldiğinde otomatik olarak oluşturulan bir dosya. Günlük verileri, tarih/saat damgası, olayın açıklaması ve bu olaya özgü bilgileri içerir. Bu dosyalar, teknik sorunlar yaşandığında sorun giderme sırasında veya veri ihlali soruşturmasında yararlıdır. Ayrıca "denetim günlüğü" veya "denetim geçmişi" olarak da adlandırılır.
Güvenli Kart Okuyucu (SCR)	Ödeme kartlarını güvenli bir şekilde kabul etmek için cep telefonuna veya tablete takılan PTS onaylı bir cihaz. PCI PTS onaylı SCR'ler, kart verilerini SRED aracılığıyla korur ve kripto şifreler. Ayrıca bkz. SRED.
Güvenlik Açığı *	Kötüye kullanılması halinde sistemin kasıtlı veya kasıtsız bir şekilde ihlal edilmesine neden olabilecek kusur veya zaaf.
Güvenlik Açığı Taraması	Bir bilgisayardaki veya ağdaki olası zayıf noktaları (güvenlik açıklarını) algılayan ve sınıflandıran bir yazılım aracı. PCI DSS Gereksinimi 11.2.2 uyarınca üç ayda bir Onaylı bir Tarama Firması tarafından bir dış harici güvenlik açığı taraması yapılmalıdır. Diğer güvenlik açığı taramaları (dahili taramalar ve ağ değişikliklerinden sonra yapılan taramalar gibi) kuruluşun BT departmanındaki nitelikli personel veya bir güvenlik hizmeti sağlayan firma (Onaylı Tarama Firması gibi) tarafından gerçekleştirilebilir. *Ayrıca bkz. Onaylı Tarama Firması (ASV).*
Güvenlik Duvarı *	Ağ kaynaklarını yetkisiz erişime karşı koruyan donanım ve/veya yazılım. Güvenlik duvarı, bir dizi kural ve diğer ölçütlere dayanarak farklı güvenlik düzeyleri olan bilgisayar veya ağlar arasındaki iletişime izin verir veya bu iletişimi reddeder.
Güvenlik Kodu *	Ödeme kartının ön yüzüne veya arka imza paneline basılı üç veya dört basamaklı bir değer. Bu kod, tek bir kartla benzersiz bir şekilde ilişkilendirilir ve genellikle kartın fiziken satış esnasında okutulmadığı işlem sırasında kartın yasal kart sahibi tarafından kullanıldığından emin olmak için ek bir kontrol olarak kullanılır. Ayrıca kart güvenlik kodu olarak da adlandırılır.
Hassas Olan Kimlik Doğrulama Verileri *	Kartın manyetik şeridinde veya çipinde saklanan, kart sahiplerinin kimliklerini doğrulamak ve/veya ödeme kartı işlemlerinin provizyonunu yapmak için kullanılan güvenlikle ilgili bilgiler.
Hizmet Sağlayan Firma *	Üye işyerlerine çeşitli hizmetler sunan bir işletme. Genellikle, bu işletmeler kart verilerini başka bir işletme (üye işyeri gibi) adına depolar, işler veya aktarır YA DA yönetilen güvenlik duvarları, sızma algılama, hosting ve BT ile ilgili başka hizmetler sağlayan yönetilen hizmet sağlayan firmalardır. Ayrıca "satıcı firma" olarak da adlandırılır.
Hosting Hizmeti Sağlayan Firma *	Müşterilerinin verilerinin hizmet sağlayıcının sunucularında "barındırıldığı" veya tutulduğu üye işyerlerine ve diğer hizmet sağlayan firmalara çeşitli hizmetler sunar. Genel hizmetler arasında, bir sunucu üzerinde birden fazla üye işyeri için ortak alan, bir üye işyerine özel bir sunucu sağlama veya "alışveriş sepeti" seçenekleri olan bir web sitesi gibi web uygulamaları yer almaktadır.
İşletim Sistemi *	Bir bilgisayar sistemi üzerindeki bilgisayar faaliyetlerinin genel yönetimini ve koordinasyonunu sağlayan yazılımlar. Örnekler arasında Microsoft Windows, Apple OSX, iOS, Android, Linux ve UNIX yer almaktadır.
Kablosuz Ödeme Terminali	Çeşitli kablosuz teknolojiler kullanarak İnternet'e bağlanan ödeme terminali.
Kart Kopyalama	Doğrudan tüketicinin ödeme kartından ya da yetkisiz taşınabilir kart okuyucusuyla veya üye işyerinin ödeme terminalinde değişiklikler yaparak üye işyerinin bir konumundaki ödeme altyapısından kart verilerini çalmak. Amacı dolandırıcılıktır, ciddi bir tehdittir ve herhangi bir üye işyerinin sistemi hedeflenebilir.
Kart Kopyalama Cihazı	Genellikle kart okuma cihazına takılan, ödeme kartından bilgileri yasadışı olarak elde etmek ve/veya depolamak için tasarlanmış olan fiziksel bir cihaz. Ayrıca "kart kopyalayıcı" olarak da adlandırılır.

Sözlük

TERİM	TANIM
Kart numarası (PAN) *	Kart sahibinin hesabını tanımlayan kredi ve hesap kartları için benzersiz numara.
Kart Verileri/Müşteri Kartı Verileri *	Kart verileri en azından kart numarasını (PAN) içerir ve kart sahibinin adını ve son kullanma tarihini de içerebilir. PAN kartın ön yüzünde görünür ve kartın manyetik şeridine ve/veya gömülü çipine kodlanmış haldedir. Ayrıca kart sahibinin verileri olarak da adlandırılır. Ayrıca, bir ödeme işleminin parçası olabilecek ancak işlem yetkisi verildikten sonra saklanmaması gereken ek veri unsurları için bkz. *Hassas Olan Kimlik Doğrulama Verileri*.
Kasa	Bkz. Elektronik Yazarkasa.
Kimlik Bilgileri	Kullanıcının sisteme erişebilmesi için kimliğini belirlemek ve doğrulamak için kullanılan bilgiler. Kimlik bilgileri genellikle kullanıcı adı ve parola gibi bilgilerdir. Kimlik bilgileri parmak izi, retina taraması veya taşınabilir bir "simge oluşturucu" tarafından oluşturulan tek seferlik sayı içerebilir. Erişim için birden çok kimlik bilgisi gerektiğinde güvenlik daha güçlü olur.
Kimlik Doğrulama *	Bilgisayara erişmeye çalışan bir kişi, cihaz veya işlemin kimliğini doğrulama yöntemi. Kimliğin/kullanıcının geçerli olduğunu onaylamak için aşağıdakilerden biri veya daha fazlası sağlanır: • Parola veya anahtar parolası (kullanıcının bildiği bir şey) • Kullanıcıya özgü bir simge, akıllı kart veya dijital sertifika (kullanıcının sahip olduğu bir şey) • Parmak izi gibi biyometrik tanımlayıcı (kullanıcının olduğu veya yaptığı bir şey)
Kötü amaçlı yazılım *	Veri çalmak ya da uygulamalara veya işletim sistemine zarar vermek amacıyla bir bilgisayar sistemine sızmak üzere tasarlanmış kötü amaçlı yazılımlar. Bu yazılımlar genellikle e-posta veya web sitelerinde gezme gibi birçok işletme tarafından onaylı etkinlik sırasında ağa girer. Kötü amaçlı yazılım örnekleri arasında virüsler, solucanlar, Truva atları, casus yazılımlar, reklam yazılımları ve korsanlık amaçlı programlar bulunur.
Kripto Şifreleme	Bilgileri, matematiksel olarak belirli bir dijital anahtarın sahipleri dışında taraflarca kullanılmayacak forma dönüştürmek için kripto yöntemi kullanma süreci. Kripto şifreleme kullanımı bilgileri, suçlular açısından değerini düşürerek korur. Ayrıca bkz. *Kripto Yöntemi.*
Kripto Şifrelenmemiş Veri	Öncelikle şifresinin çözülmesine gerek kalmadan okunabilen herhangi bir veri. Ayrıca "düz metin" ve "açık metin" verileri olarak da adlandırılır.
Kripto Yöntemi	Kripto yöntemi, verileri bir insan veya bilgisayar tarafından okunamaz hale getirerek koruma yöntemidir. Kripto yöntemi, yalnızca amaçlanan alıcı, yalnızca gönderen ve alıcının bildiği bir yöntem kullanarak verileri tekrar okunabilir hale getirebildiğinde yararlıdır. Ayrıca bkz. *Kripto Şifreleme*.
Küçük Ölçekli Üye İşyeri	Küçük ölçekli bir üye işyeri genellikle bağımsız idare edilen ve işletilen, tek ya da birkaç konuma sahip olan ve BT bütçesi sınırlı olan ya da hiç olmayan ve genellikle BT personeli istihdam etmeyen bir işletmedir. Küçük ölçekli bir üye işyerinin PCI uyumunu doğrulamasının gerekli olup olmadığı, kredi kartı firması veya POS hizmeti veren banka (üye işyeri bankası) tarafından belirlenir.
Mobil Cihaz	Küçük ve taşınabilir olan, bilgisayar ağlarına kablosuz olarak bağlanabilen akıllı telefonlar ve tabletler gibi cihazlar.

Sözlük

TERİM	TANIM
Mobil Ödeme Kabulü	Ödeme işlemlerini kabul etmek ve işlemek için mobil cihazların kullanılması. Mobil cihaz genellikle piyasada bulunan bir kart okuyucu aksesuarı ile eşleştirilir.
Nitelikli Güvenlik Denetmeni (QSA) *	Bir kuruluşun PCI DSS gereksinimlerine uyumunu doğrulamak amacıyla PCI Güvenlik Standartları Konseyi tarafından onaylanan bir şirket.
Ödeme Ara Yazılımı	İki veya daha fazla, birbiriyle alakalı olmayabilen ödeme uygulamalarını birbirine bağlayan yazılımlar için kullanılan genel bir terim. Örneğin, bir ödeme terminalindeki bir uygulama ile bir işlemciye kart verileri gönderen başka bir üye işyeri sistemi arasında kart verileri alışverişi yapabilir.
Ödeme İşleyici *	Üye işyerleri tarafından, kendi adına ödeme kartı işlemlerini gerçekleştirmek için kullanılan kuruluş. Ödeme işleyicileri genellikle POS hizmeti verse de kredi kartı firması tarafından tanımlanmadıkça POS hizmeti veren banka (üye işyeri bankası) olarak görülmez. Ayrıca "ödeme aracılığı yapan kuruluş" veya "ödeme hizmeti sağlayan firma" (PSP) olarak da adlandırılırlar. Ayrıca bkz. *Üye İşyeri Bankası*.
Ödeme Sistemi	Bir üye işyerinin perakende konumunda (satış noktaları/mağazalar ve e-ticaret mağazaları dahil) kart ödemelerini kabul etme sürecinin tamamını kapsar ve bir ödeme terminali, elektronik yazarkasa, ödeme terminaline bağlı diğer cihaz veya sistemler (örneğin, bağlantı için Wi-Fi veya envanter için kullanılan bir bilgisayar), ödeme sayfaları gibi e-ticaret bileşenleri olan sunucular ve bir üye işyeri bankasına bağlantıları içerebilir.
Ödeme Sistemi Satan Firma	Bir üye işyerine tam bir ödeme çözümü satan, lisanslayan veya dağıtan bir satıcı firma. Çözüm, satış noktası içindeki ödemeleri işlemek için gereken donanım ve yazılımı kapsar ve bir ödeme işlemcisine bağlanma yöntemi sağlar.
Ödeme Terminali	Müşterilerin kartla yaptıkları ödemeleri kaydırarak, cihazdaki yuvaya sokarak, takarak ya da dokunarak okutma yoluyla kabul etmek için kullanılan donanım cihazı. Ayrıca "satış noktası (POS) terminali", "kredi kartı makinesi" veya "PDQ terminali" olarak da adlandırılır.
Ödeme Uygulaması *	PA-DSS ile ilgili, ödeme işlemlerinin provizyonı veya mutabakatının bir parçası olarak kart sahiplerinin verilerini depolayan, işleyen veya ileten bir yazılım uygulaması.
Ödeme Uygulaması Satan Firma	Ödeme işlemleri sırasında kart verilerini depolayan, işleyen ve/veya aktaran uygulamaları satan firma.
Onaylı Tarama Firması (ASV) *	PCI Güvenlik Standartları Konseyi tarafından sistem yapılandırmasındaki genel zaafları belirlemek için harici güvenlik açığı tarama hizmetleri yürütmek üzere onaylanan firma.
Öz Değerlendirme Anketi (SAQ) *	Kuruluşun kendisi tarafından bu gereksinimleri karşıladığını teyit etmek için doldurulan bir dizi PCI DSS gereksinimini kapsayan bir anket.
P2PE	PCI Güvenlik Standartları Konseyi'nin Noktadan Noktaya Kripto Şifreleme standardının kısaltması. Ayrıntılar için bkz. www.pcisecuritystandards.org
PA-DSS *	PCI Güvenlik Standartları Konseyi'nin Ödeme Uygulaması Veri Güvenliği Standardının kısaltması. Ayrıntılar için bkz. www.pcisecuritystandards.org

Sözlük

TERİM	TANIM
Parola *	Kullanıcının kimliğini doğrulamak için kullanılan bir sözcük, ifade veya karakter dizgesi. Kullanıcı adıyla birleştirildiğinde parola, bilgisayar kaynaklarına erişim sağlamak amacıyla kullanıcının kimliğini kanıtlamak için tasarlanmıştır.
PCI *	Ödeme Kartları Endüstrisinin kısaltması.
PCI DSS *	PCI Konseyi'nin "Ödeme Kartları Endüstrisi Veri Güvenliği Standardının" kısaltması. Ayrıntılar için bkz. www.pcisecuritystandards.org
PCI DSS Onaylı	Yürürlükteki tüm PCI DSS gereksinimlerinin tek bir zamanda karşılandığının kanıtı. Belirli bir üye işyeri bankasının ve/veya kredi kartı firmasının gereksinimlerine bağlı olarak onaylama, yürürlükteki PCI DSS Öz Değerlendirme Anketi veya yerinde değerlendirmeyle oluşturulan Uyum Raporu üzerinden gerçekleştirilebilir.
PCI DSS Uyumlu	Mevcut PCI DSS'nin yürürlükteki tüm gereksinimlerini, olağan iş süreçleri yaklaşımı ile sürekli olarak karşılar. Uyum, tek bir zamanda değerlendirilip doğrulanır; ancak güçlü bir güvenlik sağlama gereksinimlerine sürekli olarak uymak üye işyerlerine kalmıştır. Üye işyeri bankaları ve/veya kredi kartı firmaları, PCI DSS uyumunu resmi olarak yıllık bazda onaylanmasını gerektirebilir.
PCI Listesinde Bulunan Noktadan Noktaya Kripto Şifreleme Çözümü	PCI Noktadan Noktaya Kripto Şifreleme (P2PE) standardına göre onaylanmış ve PCI Konseyinin web sitesinde listelenen kripto şifreleme çözümü.
PCI Onaylı Ödeme Terminali	PCI PIN İşlem Güvenliği (PTS) standardına göre onaylanmış ve PCI Konseyinin web sitesinde listelenen ödeme terminali.
PCI Onaylı Ödeme Uygulaması	PCI Ödeme Uygulamaları Veri Güvenliği Standardı (PA-DSS) uyarınca onaylanmış ve PCI Konseyinin web sitesinde listelenen yazılım uygulaması.
PED *	"PIN giriş cihazı" kısaltması. Müşterinin PIN kodunu girdiği tuş takımı. Ayrıca "PIN tuş takımı" olarak da adlandırılır.
PIN *	"Kişisel kimlik numarası" kısaltması. Yalnızca kullanıcının ve sistemin bildiği, kullanıcının sistemdeki kimlik doğrulaması için kullanılan benzersiz bir sayı. Genellikle PIN'ler, nakit avans işlemleri için bankamatiklerde veya kart sahibinin imzasının yerine geçmek üzere EMV çip kartlarında kullanılır. PIN'ler, kart sahibinin kartı kullanma yetkisi olup olmadığını belirlemeye ve kartın çalınması halinde yetkisiz kullanımını önlemeye yardımcı olur.
POS Hizmeti Veren Banka *	Bkz. *Üye İşyerinin Çalıştığı Bankave Ödeme İşleyici*.
Provizyon *	Bir ödeme kartı işleminde, POS hizmeti veren banka işlemi kredi kartını veren firma/ödeme işleyici ile doğruladıktan sonra bir üye işyeri işlem onayı aldığında, provizyon oluşur.
PTS *	PCI Konseyi'nin PIN İşlem Güvenliği standardının kısaltması. PTS, PIN kabulü etkileşim noktası (POI) terminallerinin modüler değerlendirme gereksinimleri setidir. Ayrıntılar için bkz. www.pcisecuritystandards.org
QIR *	"Nitelikli Entegre Edici ya da Satıcı" kısaltması. QIR'ler, PCI Güvenlik Standartları Konseyi tarafından üye işyerlerinin ödeme sistemlerinin kurulumu sırasında kritik güvenlik kontrollerini ele almak için özel olarak eğitilmiş entegre ediciler ve satıcılardır. Ayrıntılar için bkz. www.pcisecuritystandards.org

Sözlük

TERİM	TANIM
Sanal Ödeme Terminali *	Sanal ödeme terminali, üye işyerinin ödeme kartı verilerini güvenli bağlantısı olan web tarayıcısı üzerinden manuel olarak girdiği, ödeme kartı işlemlerinin provizyonu için POS hizmeti veren banka, işleyici veya üçüncü taraf hizmet sağlayan firma web sitesine web tarayıcı tabanlı erişimdir. Fiziksel terminallerin aksine sanal ödeme terminalleri verileri doğrudan bir ödeme kartından okumaz. Üye işyeri genellikle ödeme kartı verilerini güvenli bağlantısı olan web tarayıcısı üzerinden manuel olarak girer. Ödeme kartı işlemleri manuel olarak girildiğinden, sanal ödeme terminalleri genellikle düşük işlem hacmi olan üye işyerlerinin sistemlerinde fiziksel terminaller yerine kullanılır.
Sanal Özel Ağ (VPN) *	İnternet üzerinden veri alışverişi yapmak ve telefon görüşmeleri gerçekleştirmek için güvenli ve özel bir kanal oluşturan yazılım.
Satıcı / Entegre Edici *	Ödeme uygulamalarını satan ve/veya entegre eden, ancak bunları geliştirmeyen kuruluş.
Satıcı firma	Bir üye işyerine işlerin seyri için gereken bir ürün veya hizmeti sağlayan işletme. Hizmet sunulduğu durumlarda satıcı firma, hizmet sağlayan firma olarak kabul edilebilir ve üye işyerinin sisteminde kart verilerinin güvenliğini etkileyebilecek şekilde fiziksel konumlara veya bilgisayar sistemlerine erişmesi gerekebilir. Ayrıca bkz. *Hizmet Sağlayan Firma*.
Siber Saldırı	Bir bilgisayara veya sisteme zorla girme amaçlı herhangi bir saldırgan eylem. Siber saldırılar, bir bilgisayara casus yazılım yükleme, kart verilerini çalmak için ödeme sistemine girme veya elektrik şebekesi gibi kritik altyapıyı bozmaya çalışmak gibi birçok şekilde karşımıza çıkabilir.
Simgeleştirme	Kart numarasının (PAN), simge adı verilen alternatif bir değerle değiştirildiği bir işlem. Kartın boş geçersiz olduğu durumlar, para iadeleri veya yinelenen faturalama gibi durumlarda işlevleri yerine getirmek için asıl PAN yerine simgeler kullanılabilir. Simgeler ayrıca kullanılamaz oldukları ve bu yüzden de suçlu için hiçbir değerleri olmadığından çalınma durumlarında daha fazla güvenlik sağlarlar.
SRED	"Güvenli Okuma ve Veri Alışverişi" kısaltması. Ödeme terminallerindeki kart verilerini korumak ve kripto şifrelemek için tasarlanmış bir dizi PCI PTS gereksinimi. PCI Konseyi Listesinde Bulunan Noktadan Noktaya Kripto Şifreleme (P2PE) çözümü, SRED etkin olan ve kart verilerinin kripto şifrelemesi etkin bir şekilde gerçekleştiren PTS tarafından onaylı ve listesinde yer alan bir ödeme terminali kullanmalıdır.
Ticari İhtiyaç Doğrultusunda Bilinmesi Gereken Bilgiler	Sistemlere veya verilere erişimin, kullanıcının ticari ihtiyaçları doğrultusunda, yalnızca kullanıcının iş fonksiyonu için gereken kadar verildiği ilke.
Üye İşyeri Bankası *	Üye İşyeri adına kredi ve/veya hesap kartıyla yapılan ödemeleri işleyen bir banka veya finans kuruluşudur. Ayrıca, "POS hizmeti veren banka", "alıcı banka", "kart işleyici" ya da "ödeme işleyici" olarak da adlandırılır. Ayrıca bkz. *Ödeme İşleyici*.
Uygulama *	Bilgisayar, akıllı telefon, tablet, dahili sunucu veya web sunucusu üzerinde çalışan yazılım programı veya programlar grubu.
Uzaktan Erişim *	Ağın dışındaki bir konumdan bir bilgisayar ağına erişim. Uzaktan erişim bağlantıları, şirketin kendi ağından veya uzak bir konumdan gelebilir. Uzaktan erişim teknolojisinin bir örneği sanal özel ağdır (VPN). Uzaktan erişim dahili (örn. BT desteği) veya harici (örn. hizmet sağlayan firmalar, üçüncü taraf aracıları, entegre ediciler/satıcılar) olabilir.

Sözlük

TERİM	TANIM
Varsayılan Parola	Yeni yazılım veya donanım ile birlikte gönderilen basit bir parola. Varsayılan parolalar (“admin” veya “şifre” ya da “123456” gibi) kolayca tahmin edilebilir ve genellikle çevrimiçi arama yaparak bulunabilir. Yer tutucu olarak tasarlanırlar ve gerçek bir güvenlik sunmazlar, bu nedenle yeni yazılım veya donanım yüklendikten sonra daha güçlü bir parolayla değiştirilmelidir.
Veri Güvenliğinin Esasları (PCI DSS)	Küçük Ölçekli Üye İşyerleri için Veri Güvenliğinin Esasları, üye işyerlerinin güvenliklerini basitleştirmelerine ve riskleri azaltmalarına yardımcı olan bir dizi eğitim kaynağı ve bir değerlendirme aracıdır. DSE, kredi kartı firmaları ve POS hizmeti veren bankalar (üye işyeri bankaları) tarafından uygun olarak belirlenen üye işyerleri için PCI DSS Öz Değerlendirme Anketlerine (SAQs) alternatif bir yaklaşım olarak tasarlanmıştır.
Veri İhlali	Veri ihlali, hassas olan verilerin yetkisiz bir tarafça örüntülenmiş, çalınmış veya kullanılmış olma ihtimalinin olduğu bir olaydır. Veri ihlallerinde, kart verileri, kişisel sağlık bilgileri (PHI), kişisel tanımlanabilir bilgiler (PII), ticari sırlar veya fikri mülkiyet vb. verilerin ihlali olabilir.
Virüs	Kendi kopyalarını “virüslü” bir bilgisayardaki diğer yazılım veya veri dosyalarına kopyalayan kötü amaçlı yazılımlar. Kendisini kopyaladıktan sonra virüse, bilgisayardaki tüm verileri silmek gibi kötü amaçlı bir yük komutu verebilir. Virüs bir süre boyunca hiçbir değişiklik yapmadan bekleyip yükünü daha sonra çalıştırabilir veya kötü amaçlı bir eylemi hiç tetikleyemeyebilir. Kendisini e-posta eki olarak veya ağ iletisinin bir parçası olarak yeniden göndererek çoğaltan virüslere “solucan” denir.
Wi-Fi *	Fiziksel kablo bağlantısı olmaksızın bilgisayarları bağlayan kablosuz ağ.
Yama *	Mevcut yazılıma işlevsellik ekleyen veya bir kusuru (veya “hata”) düzelten güncelleme.
Yinelenen Ödeme	Üye işyerlerinin, aylık üyelikler veya abonelikler gibi zaman içinde müşterilerine tekrar tekrar fatura gönderdiği bir faturalandırma yöntemi. Bunu yapmanın güvenli bir yolu, POS hizmeti veren bankanın/işleyicinin kart verilerinin simgeleştirilmesidir; bu işlem, verilerin korunmasını sağlar ve üye işyerini bu sorumluluktan kurtarır.
Yönlendirici *	İki veya daha fazla dahili veya harici bilgisayar ağını bir ağ üzerinden “yönlendirmek” veya kılavuzluk etmek ve verilerin bu ağlar arasında sorunsuz akmasını sağlamak için bağlayan donanım veya yazılım. Yönlendirici ayrıca, yalnızca onaylanmış trafiğe izin verip onaylanmamış trafiği reddederek daha fazla güvenlik sağlayabilir.