Payment Card Industry (PCI) (Ödeme Kartı Endüstrisi (PCI))
Veri Güvenliği Standardı (DSS) ve Ödeme Uygulaması Veri Güvenliği Standardı (PA-DSS)

Terimler, Kısaltmalar ve Kısa Adlar Sözlüğü

Sürüm 3.0

Ocak 2014

Terim	Tanım
AAA	“Kimlik doğrulama, yetkilendirme ve kullanıcı yönetimi” kelimeleri için kısa ad. Bir kullanıcının doğrulanabilir kimliğini esas alan kimlik doğrulamaya, kullanıcı haklarını esas alan yetkilendirmeye ve ağ kaynakları tüketimine yönelik hesap yönetimi protokolü.
Adli İnceleme	“Adli bilişim” olarak da anılır. Bilgi güvenliği ile ilgili olarak, veri ihlallerinin nedenini belirlemek için bilgisayar kaynaklarından delil toplamak amacıyla inceleme araçlarının ve analiz tekniklerinin uygulanması.
AES	“Gelişmiş Şifreleme Standardı”nın kısaltması. Kasım 2001'de NIST tarafından U.S. FIPS PUB 197 (veya “FIPS 197”) olarak benimsenen simetrik anahtar kriptografisinde kullanılan blok şifreleme. Bkz. *Güçlü Kriptografi.*
Ağ	Fiziksel ya da kablosuz araçlar aracılığıyla birbirine bağlanan iki ya da daha fazla bilgisayar.
Ağ Bileşenleri	Bunlarla sınırlı olmamak kaydıyla, güvenlik duvarları, anahtarlar, yönlendiriciler, kablosuz erişim noktaları, ağ cihazları ve diğer güvenlik cihazlarını içerir.
Ağ Bölümleme	Ayrıca “bölümleme” ya da “yalıtım” olarak da anılır. Ağ bölümlemesi kart sahibi verilerini depolayan, işleyen veya ileten sistem bileşenlerini diğer sistem bileşenlerinden ayırır. Uygun ağ bölümlemesi, kart sahibi veri ortamının kapsamını daraltarak PCI DSS değerlendirmesinin kapsamını da daraltmış olur. Ağ bölümlemesine yönelik kılavuz için *PCI DSS Gereksinimleri ve Güvenlik Değerlendirme Prosedürleri* bölümündeki Ağ Bölümlemesi kısmına bakın. Ağ bölümlemesi bir PCI DSS gerekliliği değildir.
Ağ Çıkış Filtrelemesi	Yalnızca açıkça izin verilen trafiğin çıkışına izin verilen, ağ dışına çıkacak trafiği filtreleme yöntemi.
Ağ Dinleme	Ayrıca “paket dinleme” ya da “dinleme” olarak da anılır. Ağ iletişimlerini pasif olarak ağ izleyen ya da toplayan, protokollerin şifresini çözen ve ilgilenilen bilgilerin içeriklerini inceleyen bir teknik.
Ağ Giriş Filtrelemesi	Yalnızca açıkça izin verilen trafiğin ağa girmesine izin verilen, iç ağ trafiği filtreleme yöntemi.
Ağ Güvenlik Taraması	Bir kuruluşun sistemlerinin manuel ya da otomatik araçlar kullanılarak güvenlik açıkları için uzaktan kontrol edildiği süreç. Dahili ve harici sistemleri araştırmayı ve ağ aracılığıyla sunulan hizmetlerle ilgili raporlamayı içeren güvenlik taramaları. Taramalar işletim sistemleri, hizmetler ve cihazlardaki kötü niyetli kişiler tarafından kullanılabilecek güvenlik açıklarını tanımlayabilir.
Ağ Şeması	Bir ağ ortamındaki sistem bileşenlerini ve bağlantılarını gösteren şema.

Terim	Tanım
Ağ Yöneticisi	Bir kuruluşta ağ yönetiminden sorumlu personel. Sorumluluklar genellikle, bunlarla sınırlı olmamak kaydıyla, ağ güvenliği, kurulumlar, güncellemeler, bakım ve izleme faaliyetlerini içerir.
Akıllı Kart	Ayrıca "çipli kart" ya da “IC kart (bütünleşik devre kartı)” olarak da anılır. İçinde bütünleşik devre bulunan ödeme kartı türü. Aynı zamanda "çip" olarak da anılan devreler, manyetik şerit verilerine eşdeğer veriler dâhil, ancak bunlarla sınırlı olmamak kaydıyla ödeme kartı verilerini içerir.
Ana Bilgisayar	Çok büyük hacimlerde veri giriş-çıkışını işlemek ve çıktı bilgi işlemini vurgulamak için tasarlanan bilgisayarlar. Ana bilgisayarlar, birden fazla bilgisayarın aynı anda çalışıyor gibi görünmesini sağlayacak şekilde birden fazla işletim sistemini çalıştırabilir. Çoğu eski sistem ana bilgisayar tasarımına sahiptir.
Ana Makine / Sistem	Bilgisayar yazılımının bulunduğu ana bilgisayar donanımı.
ANSI	“Amerikan Ulusal Standartlar Enstitüsü”nün kısaltması. ABD'deki gönüllü standardizasyon ve uygunluk değerlendirme sistemini idare ve koordine eden özel, kâr amacı gütmeyen kuruluş.
AOC	“Uyum onayı belgesi” için kısa ad. AOC, Öz Değerlendirme Anketi’nde veya Uyumluluk Raporu'nda belgelendiği gibi üye iş yerlerinin ve hizmet sağlayıcıların PCI DSS değerlendirme sonuçlarını belgelendirmesine yönelik bir formdur.
AOV	“Geçerlilik belgesi” için kısa ad. AOV, PA-QSA’lar için PA-DSS Geçerlilik Raporu'nda belgelendiği gibi, PA-DSS değerlendirme sonuçlarının onaylanmasına yönelik bir formdur.
Aracı Kurum/ Entegratör	Ödeme uygulamalarını satan ve/veya entegre eden, ancak geliştirme yapmayan kuruluş.
ASV	"Onaylı Tarama Hizmeti Sağlayıcı" için kısa ad. Dış zafiyet tarama hizmetleri vermek üzere PCI SSC tarafından onaylanmış şirket.
Ayrıcalıklı Kullanıcı	Temel erişim ayrıcalıklarından daha fazla ayrıcalıklara sahip herhangi bir kullanıcı hesabı. Genellikle, bu hesaplar standart bir kullanıcı hesabından daha fazla hak içeren, yükseltilmiş ya da artırılmış ayrıcalıklara sahiptir. Ancak, farklı ayrıcalıklı hesaplar arasında ayrıcalıkların kapsamı, kuruluşa, iş görevine ya da rolüne ve kullanılan teknolojiye bağlı olarak dikkate değer ölçüde farklılık gösterebilir.
Bağımlılık	PA-DSS bağlamında bağımlılık, ödeme uygulamasının PA-DSS gereksinimlerini karşılaması için gerekli bir yazılım veya donanım bileşenidir (bir donanım terminali, veritabanı, işletim sistemi, API, kod kütüphanesi vb. gibi) .
Bağlantı Noktası	Ağlar arasındaki iletişimi kolaylaştırmak için belirli bir iletişim protokolüyle ilişkilendirilen mantıksal (sanal) bağlantı noktaları.

Terim	Tanım
Barındırma Hizmeti Sağlayıcısı	Üye iş yerlerine ve diğer hizmet sağlayıcılara çeşitli hizmetler sunar. Hizmetler bir sunucu üzerinde yer alan paylaşılan alandan "alışveriş sepeti" seçeneklerinin tamamına; ödeme uygulamalarından ödeme geçitlerine ve işlemcilere bağlantılara ve her sunucu başına yalnızca bir müşteriye özel barındırmaya kadar basitten karmaşığa değişkenlik gösterir. Bir barındırma hizmeti sağlayıcısı, tek sunucuda birden fazla kuruluşu barındıran, paylaşılan bir barındırma hizmeti sağlayıcısı olabilir.
BAU	"İşin olağan akışı" için kısa ad. BAU, bir kuruluşun normal günlük iş operasyonlarıdır.
Belirteç	Kimlik doğrulama ve erişim kontrolü bağlamında, belirteç, dinamik veya iki öğeli kimlik doğrulama yapmak amacıyla bir kimlik doğrulama sunucusuyla veya VPN ile birlikte çalışan donanım ya da yazılım tarafından sağlanan bir değerdir. Bkz. *RADIUS, TACACS,* ve *VPN.*
Bellek Ayıklama Saldırıları	Bellekte bulunan verileri işlem görüyormuş ya da düzgün bir biçimde temizlenmemiş veya üzerine yazılmıyormuş gibi inceleyip ayıklayan kötü amaçlı yazılım etkinliği.
Bilgi Güvenliği	Gizliliği, bütünlüğü ve erişilebilirliği güvence altına alan bilgi koruma işlemi.
Bilgi Sistemi	Bilginin toplanması, işlenmesi, bakımının sağlanması, kullanılması, paylaşılması, yayılması veya imhası için düzenlenen, ayrı bir yapılandırılmış veri kaynakları bütünü.
Bluetooth	Verilerin kısa mesafelerde iletilmesini kolaylaştırmak için kısa mesafeli iletişim teknolojisi kullanılan kablosuz protokol.
Bölünmüş Bilgi	İki ya da daha fazla kuruluşun ayrı ayrı, ortaya çıkan kriptogtafik anahtara ilişkin hiçbir bilgiyi tek tek taşımayan temel bileşenlere sahip olmasını sağlayan yöntem.
Casus Yazılım	Kurulduğunda kullanıcının bilgisayarını, kullanıcının izni olmaksızın ele geçiren ya da kısmen kontrol altına alan kötü niyetli yazılım türü.
CDE	"Kart sahibi veri ortamı" için kısa ad. Kart sahibi verilerini veya hassas kimlik doğrulama verilerini kaydeden, işleyen veya ileten kişiler, işlemler ve teknoloji.
CERT	Carnegie Mellon Üniversitesi "Bilgisayar Acil Durum Müdahale Ekibi"nin kısa adı. CERT Programı, ağ sistemlerinde saldırıları engellemek, hasarı sınırlamak ve kritik hizmetlerin sürekliliğini sağlamak üzere uygun teknoloji ve sistem yönetimi uygulamalarının kullanımını geliştirip hayata geçirir.
CIS	"İnternet Güvenliği Merkezi" için kısa ad. Kurumların yetersiz teknik güvenlik kontrollerinden kaynaklanan iş ve e-ticaret kesintisi riskini azaltmaya yardımcı olma görevini üstlenen, kâr amacı gütmeyen kuruluşlar.
CVSS	"Genel Güvenlik Açığı Puanlama Sistemi" için kısa ad. Bilgisayar sisteminin güvenlik açıklarının ciddiyetini yaymak ve yanıtın aciliyeti ile önceliğini belirlemeye yardımcı olmak için tasarlanan, bağımsız danışmanlar tarafından geliştirilen, tüm sektöre açık standart. Daha fazla bilgi için bkz. *ASV Program Rehberi*.

Terim	Tanım
Değişiklik Kontrolü	Kurulumdan önce sistemlerdeki ve yazılımlardaki değişikliklerin etkilerinin gözden geçirilmesi, test edilmesi ve onaylanmasına yönelik süreçler ve prosedürler.
Denetim Günlüğü	"Denetim izi" olarak da anılır. Sistem etkinliklerinin kronolojik kaydı. Başlangıçtan nihai sonuçlara kadar bir işlemde operasyona, prosedüre veya olaya neden olan ya da işlemi çevreleyen ortamların ve aktivitelerin sırasının incelenmesine, gözden geçirilmesine ve yeniden yapılandırılmasına izin vermek için yeterli düzeyde bağımsız olarak doğrulanabilen bir iz sağlar.
Denetim İzi	Bkz. *Denetim İzi.*
Dinamik Paket Filtreleme	Bkz. *Durum Denetimi.*
Disk Şifreleme	Bir cihaza (örneğin sabit disk ya da flaş bellek) kaydedilen tüm verileri şifrelemek için kullanılan teknik veya teknoloji (yazılım ya da donanım). Alternatif olarak, belirli dosyaların veya sütunların içeriklerini şifrelemek için *Dosya Düzeyinde Şifreleme* veya *Sütun Düzeyinde Veritabanı Şifreleme* kullanılır.
Dizin Belirteci	Öngörülemeyen bir değer için belirli bir dizin esas alındığında, PAN'ın yerini alan bir kriptografik belirteç.
DMZ	“Tampon bölge”nin kısaltması. Bir kuruluşun dâhili özel ağına ek bir güvenlik katmanı sağlayan fiziksel veya mantıksal alt ağ. DMZ, internet ile kuruluşun iç ağı arasına ek bir güvenlik ağı katmanı ekler. Böylece dış tarafların tüm iç ağ yerine yalnızca DMZ'de yer alan cihazlara doğrudan bağlantısı olur.
DNS	“Alan adı sistemi” veya “Alan adı sunucusu” için kısa ad. İnternet gibi ağlardaki kullanıcılara ad çözümlemesi hizmetleri sunmak için dağıtılmış bir veritabanındaki alan adlarıyla ilişkili bilgileri kaydeden bir sistem.
Dolgu	Kriptografide tek seferlik dolgu, rastgele bir anahtar ya da düz metin kadar uzun olan ve yalnızca bir kez kullanılan "dolgu" ile birleştirilmiş metin içeren bir şifreleme algoritmasıdır. Ek olarak, anahtar gerçekten rastgele seçilmiş, asla yeniden kullanılmamış ve gizli tutulmuş ise tek seferlik dolgu kırılamaz niteliktedir
Dosya Bütünlüğü İzleme	Belirli dosya veya logların değişikliğe uğrayıp uğramadıklarını tespit etmek için izlendiği teknik ya da teknoloji. Kritik dosyalar veya loglar değiştirildiğinde, ilgili güvenlik personeline uyarılar gönderilmelidir.
Dosya Düzeyinde Şifreleme	Belirli dosyaların tüm içeriklerinin şifrelenmesi için kullanılan teknik veya teknoloji (yazılım ya da donanım). Alternatif olarak, bkz. *Disk Şifreleme* veya *Sütun Düzeyinde Veritabanı Şifreleme.*
DSS	“Veri Güvenliği Standardı" için kısa ad. Bkz. *PA-DSS* ve *PCI DSS.*
Durum Denetimi	Ayrıca “dinamik paket filtreleme” olarak da adlandırılır. Ağ bağlantılarının durumunu izleyerek gelişmiş güvenlik sunan güvenlik duvarı özelliği. Çeşitli bağlantılar için uygun paketleri ayıracak şekilde programlanmıştır, güvenlik duvarı yalnızca kurulan bağlantıyla eşleşen paketlere izin verir, diğerlerinin tümü reddedilir.

Terim	Tanım
ECC	“Eliptik Eğri Kriptografisi” için kısa ad. Sınırlı alanlar üzerindeki eliptik eğrileri esas alan genel anahtar kriptografisi yaklaşımı. Bkz. *Güçlü Kriptografi.*
En Düşük Ayrıcalık	Rolleri ve iş görevinin sorumluluklarını yerine getirmek için gerekli olan en düşük erişim ve/veya ayrıcalıklara sahip olma.
Erişim Kontrolü	Bilgi veya bilgi işlem kaynaklarına sadece yetkili kişilerin ve uygulamaların erişmesini sağlayan mekanizmalar.
FIPS	“Federal Bilgi İşleme Standartları” için kısa ad. A.B.D. Federal Hükümeti tarafından genel olarak tanınan standartlar; aynı zamanda sivil toplum örgütleri ve taşeronların kullanımına da yöneliktir.
FTP	“Dosya Aktarım Protokolü” için kısa ad. Bir bilgisayardan diğerine internet gibi bir genel ağ aracılığıyla veri aktarmak için kullanılan ağ protokolü. FTP, şifreler ve dosya içerikleri korunmasız ve açık metin olarak gönderildiğinden, yaygın biçimde güvenli olmayan bir protokol olarak görülür. FTP, SSH veya başka teknoloji aracılığıyla güvenli olarak uygulanabilir. Bkz. *S-FTP*.
Genel Ağ	Telekomünikasyon sağlayıcı tarafından kamuya açık erişim için özel olarak veri iletim hizmeti sunmak amacıyla kurulan ve işletilen ağ. Genel ağlardaki veriler, aktarım sırasında kesilebilir, değiştirilebilir ve/veya başka yöne çevrilebilir. PCI DSS kapsamındaki genel ağlara bunlarla sınırlı olmamak kaydıyla internet, kablosuz ve mobil teknolojiler örnek olarak verilebilir.
Girdi Değişkeni	Tek yönlü bir karma işlevi uygulamadan önce kaynak verilerle art arda bağlanan rastgele veri dizesi. Giriş değişkenleri şifre kırma saldırılarının etkisini azaltmaya yardımcı olabilir. Ayrıca bkz. *Karma İşlevi* ve *Şifre Kırma Tabloları.*
Gizlilik İhlali	Ayrıca "veri gizlilik ihlali" veya "veri güvenlik açığı" olarak da anılır. Bilgisayar sisteminde kart sahibi verilerinin yetkisiz ifşa/hırsızlık, değişiklik veya tahribata maruz kalmasından şüphelenildiği saldırı.
Görevler Ayrılığı	Tek bir kişinin işlemi bozmasını engellemek için bir görevdeki adımları, farklı kişiler arasında bölüştürme uygulaması.
GPRS	“Genel Paket Radyo Hizmeti” için kısa ad. GSM cep telefonu kullanıcıları için sunulan mobil veri hizmeti. Sınırlı bant genişliğinin verimli kullanımı olarak tanınır. Özellikle e-posta ve web tarama gibi küçük miktarlarda veri gönderimi ve alımı için uygundur.
GSM	“Mobil İletişim İçin Küresel Sistem”in kısa adı. Cep telefonları ve şebekelerine yönelik popüler standart. GSM standardının aynı anda her yerde bulunması, abonelerin telefonlarını dünyanın pek çok yerinde kullanmasını sağladığından, uluslararası dolaşımı cep telefonu operatörleri arasında son derece yaygın bir hale getirmektedir.

Terim	Tanım
Güçlü Kriptografi	Güçlü anahtar uzunlukları (en az 112 bitlik etkili anahtar gücü) ve uygun anahtar yönetimi uygulamalarıyla birlikte sektör testleri yapılan ve kabul edilen algoritmaları esas alan kriptografi. Kriptografi, veriyi korumak için kullanılan ve hem şifreleme (geri dönüşlü) hem de karma işlevine (geri dönüşü olmayan ya da "tek yönlü") sahip olan bir yöntemdir. Yayın sırasında, en düşük şifreleme gücü için sektör testleri yapılan ve kabul edilen standartlar ve algoritmalara AES (128 bit ve üzeri), TDES (en az üç kat uzunlukta anahtarlar), RSA (2048 bit ve üzeri), ECC (160 bit ve üzeri) ve ElGamal (2048 bit ve üzeri) örnek olarak verilebilir. Kriptografik anahtar güçleri ve algoritmaları hakkında daha fazla bilgi için bkz. NIST Özel Yayını 800-57 1. Bölüm. (http://csrc.nist.gov/publications/).
Güvenilir Ağ	Bir kuruluşun denetim ya da yönetim yeteneği içinde yer alan kuruluş ağı.
Güvenilmeyen Ağ	Bir kuruluşa ait olan ağların dışında, kuruluşun denetim ya da yönetim yeteneği dışında bulunan ağ.
Güvenli Kodlama	Tahrif ve/veya ihlâle karşı dirençli uygulamalar oluşturma ve uygulama işlemi.
Güvenli Kriptografik Cihaz	Kriptografik işlemleri gerçekleştiren süreçler (kriptografik algoritmalar ve anahtar oluşturma dâhil) ve tanımlı bir kriptografik sınır dâhilinde bulunan donanım, yazılım ve donanım yazılımı bütünü. Güvenli kriptografik cihazlara PCI PTS ile geçerlenen ana sunucu/donanım güvenlik modülleri (HSM'ler) ve etkileşim noktası cihazları (POI'lar) örnek olarak verilebilir.
Güvenli Olmayan Protokol/Hizmet/Bağlantı Noktası	Gizlilik ve/veya bütünlük kontrollerinin bulunmamasından dolayı güvenlik sorunları çıkaran bir protokol, hizmet veya bağlantı noktası. Bu güvenlik endişeleri, internet üzerinden açık metin halinde verileri veya kimlik doğrulama bilgilerini (örneğin şifre/parola) ileten ya da varsayılan olarak veya yanlış yapılandırıldıysa suiistimale kolayca izin veren hizmetleri, protokolleri ya da bağlantı noktalarını içerir. Güvenli olmayan hizmetlere, protokoller veya bağlantı noktaları, bunlarla sınırlı olmamak kaydıyla, FTP, Telnet, POP3, IMAP ve SNMP v1 ve v2 örnek verilebilir.
Güvenli Silme	Ayrıca "güvenli temizleme" olarak adlandırılır. Geri alınamayan verileri derleyerek bir sabit sürücüde veya başka dijital ortamda bulunan verilerin üzerine yazma yöntemi.
Güvenlik Açığı	Suiistimal edilirse sistemin kasten ya da yanlışlıkla tahrif olmasına yol açabilen kusur veya zayıflık.
Güvenlik Duvarı	Ağ kaynaklarını yetkisiz erişimden koruyan donanım ve/veya yazılım teknolojisi. Bir güvenlik duvarı, kurallar ve diğer kriterler bütününe bağlı olarak, farklı güvenlik seviyesindeki ağlar arasındaki bilgisayar trafiğine izin verir veya bunu reddeder.
Güvenlik Görevlisi	Bir kuruluşun güvenlikle ilgili hususlarından birinci derecede sorumlu kişi.
Güvenlik Olayı	Bir kuruluş tarafından bir sistem veya sistemin ortamında potansiyel güvenlik çıkarımları olabileceğini değerlendirdiği bir vaka. PCI DSS bağlamında, güvenlik olayları şüpheli ya da anormal etkinliği tanımlar.

Terim	Tanım
Güvenlik Politikası	Bir kuruluşun hassas bilgileri nasıl yöneteceğini, koruyacağını ve dağıtacağını düzenleyen yasalar, kurallar ve uygulamalar bütünü.
Güvenlik Protokolleri	Veri iletimini güvenlik altına almak için tasarlanan ağ iletişimi protokolleri. Güvenlik protokollerine bunlarla sınırlı olmamak kaydıyla, SSL/TLS, IPSEC, SSH, HTTPS vb. örnek olarak verilebilir.
Hassas Bölge	Kart sahibi bilgilerini depolayan, işleyen ya da yayan sistemlerin bulunduğu herhangi bir veri merkezi, sunucu odası veya alan. Buna perakende satış mağazalarındaki kasa alanları gibi yalnızca satış noktası terminallerinin bulunduğu alanlar dahil değildir.
Hassas Kimlik Doğrulama Verileri	Kart sahiplerinin kimliğini doğrulamak ve/veya ödeme kartı işlemlerini yetkilendirmek için kullanılan güvenlikle ilgili bilgilerdir. (Bunlarla sınırlı olmamak kaydıyla, kart geçerleme kodu/değerleri, tam izleme verileri (manyetik şeritte ya da benzeri bir çipte yer alan), PIN'ler ve PIN blokları).
Hesap Numarası	Bkz. *Ana Hesap Numarası (PAN).*
Hesap Verileri	Hesap verileri kart sahibi verileri ve/veya hassas kimlik doğrulama verilerinden oluşur. Bkz. *Kart Sahibi Verileri* ve *Hassas Kimlik Doğrulama Verileri.*
Hizmet Kodu	İzleme verilerinde ödeme kartının son kullanma tarihinin ardından gelen, manyetik şeritte bulunan üç ya da dört basamaklı değer. Hizmet nitelikleri, uluslararası ve ulusal değişimler arasında farklılaştırma ya da kullanım sınırlamalarını belirleme gibi çeşitli şeyler için kullanılır.
Hizmet Sağlayıcı	Ödeme markası olmayan, başka bir kuruluş adına kart sahibi verilerini işleme, depolama ya da aktarmayla doğrudan ilgili olan iş kuruluşu. Bu aynı zamanda, kart sahibi verilerinin güvenliğini kontrol eden ya da etkileyebilecek hizmetler sunan şirketleri de içerir. Yönetilen güvenlik duvarları, IDS, diğer hizmetlerin yanı sıra barındırma hizmeti sağlayıcıları ve diğer kuruluşlar örnek olarak verilebilir. Bir kuruluş *yalnızca* genel ağ erişimi tedarikiyle ilgili bir hizmet (yalnızca iletişim bağlantısı sağlayan bir telekomünikasyon şirketi gibi) söz konusu hizmet için hizmet sağlayıcı sayılmaz (diğer hizmetler için hizmet sağlayıcı sayılabildiği halde).
HSM	“Donanım güvenlik modülü” veya “ana sistem güvenlik modülü” için kısa ad. Kriptografik anahtar yönetimi işlevleri ve/veya hesap verilerinin şifrelerinin çözülmesi için kullanılan ve güvenli bir kriptografik hizmet bütünü sağlayan fiziksel ve mantıksal olarak korumalı donanım cihazı.
HTTP	“ Bağlantılı metin aktarım protokolü” için kısa ad. Bilgileri World Wide Web üzerinde aktarmak veya iletmek için kullanılan açık internet protokolü.
HTTPS	“Güvenli yuva katmanı üzerinden bağlantılı metin aktarım protokolü” için kısa ad. Web tabanlı girişler gibi güvenlik açısından hassas iletişim için tasarlanan, World Wide Web’de kimlik doğrulama ve şifreli iletişim sağlayan güvenli HTTP.

Terim	Tanım
Hücresel Teknolojiler	Mobil İletişim için Küresel Sistem (GSM), Kod Bölmeli Çoklu Erişim (CDMA) ve Genel Paket Radyo Hizmeti (GPRS) dâhil, ancak bunlarla sınırlı olmamak kaydıyla kablosuz telefon şebekeleri aracılığıyla yapılan mobil iletişim.
IDS	"Saldırı tespit sistemi" için kısa ad. Ağ veya sistem anormalliklerini ya da yetkisiz giriş girişimlerini belirlemek ve bunlarla ilgili uyarı vermek için kullanılan yazılım veya donanım. Şunlardan oluşur: Güvenlik olaylarını üreten sensörler; olayları ve uyarıları izleyen ve sensörleri kontrol eden bir konsol; bir veritabanındaki sensörlerle loglanan olayları kaydeden merkezi bir motor. Tespit edilen güvenlik olaylarına yanıt olarak uyarılar üretmek için kurallar sistemi kullanır. Bkz. *IPS*
IETF	"İnternet Mühendisliği Görev Gücü" için kısa ad. İnternetin mimarisinin gelişimi ve sorunsuz çalışmasıyla ilgilenen, ağ tasarımcıları, operatörler, tedarikçi firmalar ve araştırmacılardan oluşan geniş, açık internet topluluğu. IETF'in resmi bir üyeliği bulunmamaktadır ve ilgi duyan herkese açıktır.
IMAP	"İnternet Mesaj Erişim Protokolü" için kısa ad. Bir e-posta istemcisinin uzak bir posta sunucusundaki e-postaya erişmesini sağlayan bir uygulama katmanı internet protokolü.
IP	"İnternet protokolü" için kısa ad. Adres bilgilerini ve paketlerin yönlendirilmesini ve kaynak ana makineden hedef ana makineye teslim edilmesini sağlayan bazı kontrol bilgilerini içeren ağ katmanı protokolü. IP, internet protokol paketindeki ana ağ katmanı protokolüdür. Bkz. *TCP*.
IP Adresi	Ayrıca "internet protokol adresi" olarak da anılır. İnternette belirli bir bilgisayarı (ana makine) benzersiz biçimde tanımlayan sayısal kod.
IP Adresi Sahtekârlığı	Ağlara veya bilgisayarlara yetkisiz erişim sağlamak için kullanılan saldırı tekniği. Kötü amaçlı kişi, mesajın güvenilir bir ana sunucudan geldiğini gösteren bir IP adresiyle bir bilgisayara aldatıcı mesajlar gönderir.
IPS	"Saldırı önleme sistemi" için kısa ad. IPS, IDS'in ötesinde yetkisiz girişi engellemek için ek bir adım daha atar.
IPSEC	"İnternet Protokolü Güvenliği" için kısaltma. Bir iletişim oturumunda tüm IP paketlerini şifreleyerek ve/veya bunların kimlik doğrulamasını yaparak ağ katmanındaki IP iletişimini güvenlik altına almaya ilişkin standart.
ISO	Yaygın biçimde "Uluslararası Standartlaştırma Örgütü" olarak bilinir. Ulusal standartlar enstitüleri ağından oluşan, devlet kuruluşu olmayan kuruluş.
İki Öğeli Kimlik Doğrulama	İki ya da daha fazla öğenin doğrulandığı bir kullanıcı kimliği doğrulama yöntemi. Bu öğeler arasında kullanıcının sahip olduğu bir şey (donanım ya da yazlım belirteci gibi), kullanıcının bildiği bir şey (şifre, parola ya da PIN gibi) veya kullanıcının yaptığı bir şey (parmak izi ya da diğer biyometrik biçimler) bulunur.

Terim	Tanım
İkili Kontrol	Hassas işlev veya bilgileri korumak için iki veya daha fazla varlığı (genelde kişileri) kullanma işlemi. Her iki varlık da korunmasız işlemlere dahil olan materyallerin fiziksel korunmasından eşit şekilde sorumludur. Tek kişinin materyallere (örneğin, kriptografik anahtara) erişmesi ve bunları kullanmasına izin verilmez. Manuel anahtar oluşturmak, iletmek, yüklemek, depolamak ve elde etmek için, ikili kontrol, anahtar bilgisinin varlıklar arasında bölünmesini gerektirir. (Ayrıca bkz. *Bölünmüş Bilgi.*)
İşlem Verileri	Elektronik ödeme kartı işlemiyle ilgili veriler.
İşletim Sistemi / İS	Tüm bilgisayar aktivitelerinin yönetimi ve koordinasyonunun yanı sıra bilgisayar kaynaklarının paylaşımından sorumlu bilgisayar sistemi yazılımı. İşletim sistemlerine Microsoft Windows, Mac OS, Linux ve Unix örnek olarak verilebilir.
İzleme	Kesintiler, alarmlar veya önceden tanımlanan diğer olaylar durumunda personeli uyarmak amacıyla bilgisayar veya ağ kaynaklarını sürekli olarak izleyen sistemlerin ve işlemlerin kullanılması.
İzleme Verileri	Ayrıca “tam izleme verileri” veya “manyetik şerit verileri” olarak da anılır. Ödeme işlemleri sırasında kimlik doğrulama ve/veya yetkilendirme için kullanılan manyetik şeride veya çipe kodlanan veriler. Bir çipteki manyetik şerit görüntüsü veya manyetik şeridin 1. hat ve/veya 2. hat kısmındaki verileri olabilir.
Joker Karakter	Bir uygulama sürümü düzeninde, tanımlı bir olası karakter alt kümesinin yerine kullanılabilecek bir karakter. PA-DSS bağlamında, joker karakterler isteğe bağlı olarak güvenliği etkilemeyen bir değişikliği göstermek için kullanılabilir. Bir joker karakter, satıcının sürüm düzeninin tek değişken öğesidir ve joker karakteri öğesinin temsil ettiği her sürüm arasında yalnızca küçük, güvenlikle ilgili olmayan değişiklikler olduğunu göstermek için kullanılır.
Kablosuz Ağlar	Bilgisayarları fiziksel bağlantı kabloları olmadan bağlayan ağ.
Kablosuz Erişim Noktası	Ayrıca “AP” olarak da anılır. Kablosuz iletişim cihazlarının kablosuz bir ağa bağlanmasını sağlayan cihaz. Genellikle kablolu ağa bağlıdır, verileri ağdaki kablosuz cihazlarla kablolu cihazlar arasında iletebilir.
Kapsam Belirleme	PCI DSS değerlendirmelerine dâhil edilecek tüm sistem bileşenlerini, kişileri ve süreçleri tanımlama işlemi. Bir PCI DSS değerlendirmesinin ilk adımı, incelemenin kapsamını doğru ve kesin bir biçimde belirlemektir.

Terim	Tanım
Karma İşlevi	Kart sahibi verilerinin *Güçlü Kriptografi aracılığıyla sabit uzunluklu bir mesaj özetine dönüştürülerek anlaşılmaz hale getirilmesi işlemi.* Karma işlevi gizli olmayan bir algoritmanın herhangi bir isteğe bağlı uzunluktaki mesajı girdi olarak alarak, sabit uzunlukta çıkış (genellikle "karma kod" veya "mesaj özeti" denir) oluşturduğu tek yönlü (matematiksel) bir işlevdir. Bir karma işlevinin aşağıdaki özelliklere sahip olması gerekir: (1) Yalnızca karma kod ile orijinal girdiyi belirlemek sayısal olarak mümkün değildir, (2) Aynı karma kodunu veren iki girdi bulmak sayısal olarak mümkün değildir. PCI DSS bağlamında, karma işlevi, karma kodunun okunamaz hale dönüştürülmesi için tüm PAN'a uygulanmalıdır. Karma işlevi uygulanan kart sahibi verilerinin, önceden hesaplanan şifre kırma saldırılarının etkililiğini azaltmak veya bitirmek için karma işlevine bir giriş değişkeni (örneğin, "güvenlik değeri") eklenmesi önerilir (bkz. *Girdi Değişkeni*).
Kart Çıkaran Kuruluş	Ödeme kartlarını çıkaran veya kart çıkaran bankalar ve kart çıkaran işleyen kuruluşlar dâhil, ancak bunlarla sınırlı olmamak kaydıyla kart çıkarma işlemlerini yapan, kolaylaştıran veya destekleyen kuruluş. Ayrıca "kart çıkaran banka" veya "kart çıkaran finans kuruluşu" olarak da anılır.
Kart çıkarma hizmetleri	Kart çıkarma hizmetleri için, bunlarla sınırlı olmamak kaydıyla kimlik doğrulama ve kart kişiselleştirme örnek olarak verilebilir.

Terim	Tanım
Kart Doğrulama Kodu veya Değeri	Kart Geçerlilik Kodu veya Değeri ya da Kart Güvenlik Kodu olarak da bilinir. Şunları belirtir: (1) Manyetik şerit verileri veya (2) basılı güvenlik özellikleri. (1) Bir kartın üzerindeki manyetik şeritte bulunan veri öğesi, şeritteki veri bütünlüğünü korumak için güvenli şifreleme işlemleri kullanır ve her türlü değişikliği veya sahteciliği ortaya çıkarır. Ödeme kartının markasına bağlı olarak CAV, CVC, CVV veya CSC olarak anılır. Aşağıdaki listede her kart markasına ait terimler sıralanmıştır: ▪ **CAV:** Kart Kimlik Doğrulama Değeri (JCB ödeme kartları) ▪ **CVC:** Kart Geçerlilik Kodu (MasterCard ödeme kartları) ▪ **CVV:** Kart Doğrulama Değeri (Visa ve Discover ödeme kartları) ▪ **CSC:** Kart Güvenlik Kodu (American Express) (2) Discover, JCB, MasterCard ve Visa ödeme kartları için, ikinci tür kart doğrulama değeri veya kodu, kartın arka yüzünde imza paneli alanında yazan, en sağdaki üç basamaklı değerdir. American Express ödeme kartları için kod, ödeme kartlarının ön yüzündeki PAN'ın üst kısmında yazılı, kabarık olmayan dört basamaklı sayıdır. Kod, her biri birbirinden ayrı bir plastik parçasıyla benzersiz biçimde ilişkilendirilmiştir ve PAN'ı plastiğe bağlar. Aşağıdaki listede her kart markasına ait terimler sıralanmıştır: ▪ **CID:** Kart Kimlik Numarası (American Express ve Discover ödeme kartları) ▪ **CAV2:** Kart Kimlik Doğrulama Değeri 2 (JCB ödeme kartları) ▪ **CVC2:** Kart Geçerlilik Kodu 2 (MasterCard ödeme kartları) ▪ **CVV2:** Kart Doğrulama Değeri 2 (Visa ödeme kartları)
Kart kabul eden Kuruluş	Aynı zamanda "üye iş yeri bankası", "kart kabul eden banka" veya "kart kabul eden finans kuruluş" olarak anılır. Ödeme kartlarının kabulü için üye iş yerleriyle ilişkileri başlatan ve sürdüren kuruluş.
Kart Kopyalayıcı	Çoğunlukla güvenli bir kart okuma cihazına takılan, bir ödeme kartından yasa dışı yollarla bilgi almak ve/veya bilgileri kaydetmek için tasarlanan fiziksel cihaz.
Kart Sahibi	Ödeme kartı tahsis edilen ya da ödeme kartını kullanma yetkisi olan herhangi bir tüketici olmayan veya tüketici konumundaki müşteri.
Kart Sahibi Verileri	Minimum olarak, kart sahibi verileri PAN'ın tamamını içerir. Kart sahibi verileri PAN'ın tamamına ek olarak şunlar olacak biçimde de görünebilir: Kart sahibi adı, son kullanma tarihi ve/veya hizmet kodu Bir ödeme işleminin parçası olarak iletilebilen veya işlenebilen (ancak kaydedilmeyen) ek veri öğeleri için bkz. *Hassas Kimlik Doğrulama Verileri*.
Kayıt	Bkz. *Denetim İzi.*

Terim	Tanım
Kırpılma	PAN verilerinin bir bölümünün kalıcı olarak kaldırılmasıyla tüm PAN'ı okunaksız hale getirmeye ilişkin yöntem. Kırpılma, dosyalarda, veri tabanlarında vb. *depolandığında* PAN'ın korunması ile ilgilidir. Ekranlarda, kağıt makbuzlarda vb. *görüntülendiğinde* PAN'ın korunması için bkz. *Maskeleme*.
Kimlik	Belli bir kullanıcı veya uygulama için tanımlayıcı.
Kimlik Doğrulama	Bir kişinin, cihazın veya işlemin kimliğinin doğrulanması işlemi. Kimlik doğrulama, genellikle aşağıdakiler gibi bir veya birden fazla kimlik doğrulama unsurunun kullanılması yoluyla meydana gelir: ▪ Şifre veya parola gibi kişinin bildiği bir şey ▪ Andaç cihazı veya akıllı kart gibi kişinin sahip olduğu bir şey ▪ Biyometrik özellikler gibi kişinin niteliği olan bir şey
Kimlik Doğrulama Bilgileri	Bir kişinin, cihazın veya işlemin kimliğini doğrulamak için kullanılan kullanıcı kimliği veya hesap kimliği ile kimlik doğrulama unsurunun/unsurlarının birleşimi,
Kişisel Güvenlik Duvarı Yazılımı	Bir tek bilgisayara kurulan güvenlik duvarı yazılımı ürünü.
Kişisel Olarak Tanımlanabilen Bilgiler	Ad, adres, sosyal güvenlik numarası, biyometrik veriler, doğum tarihi vb. dâhil ancak bunlarla sınırlı olmamak kaydıyla bir kişinin kimliğini tanımlamak veya izlemek için kullanılabilen bilgiler.
Konsol	Bir ağ ortamında sunucunun, ana sistem bilgisayarının veya başka bir sistem türünün erişimini ve kontrolünü sağlayan ekran ve klavye.
Konsol Dışı Yönetim Erişimi	Sistem bileşenine doğrudan, fiziksel bir bağlantı yerine bir ağ arayüzü üzerinden meydana gelen mantıksal sistem yöneticisi erişimini ifade eder. Konsol dışı yönetim erişimi, yerel/dahili ağlardan erişimin yanı sıra harici veya uzak ağlardan erişimi de içerir.
Kök Kullanıcı Takımı (işletim sisteminde arka planda çalışan gizli program veya programlar grubu)	Yetkisiz olarak yüklendiğinde, varlığını gizleyebilen ve bir bilgisayar sisteminin yönetim kontrolünü ele geçirebilen kötü amaçlı yazılım türü.
Kötü Amaçlı Yazılımlar / Kötücül Yazılımlar	Sahibin verilerinin, uygulamalarının veya işletim sisteminin gizliliğini, bütünlüğünü ya da erişilebilirliğini tehlikeye atmak amacıyla sahibin bilgisi veya rızası olmadan bir bilgisayar sistemine sızmak veya hasar vermek için tasarlanan yazılımlar ya da donanım yazılımları. Bu tür yazılımlar bir ağa şirketin onayladığı birçok faaliyet sırasında girer, bu da sistem güvenlik açıklarının suiistimaline yol açar. Virüsler, solucanlar, Truvalar (ya da Truva atları), casus yazılımlar, reklam yazılımları ve kök kullanıcı takımları (işletim sisteminde arka planda çalışan gizli programlar) örnek olarak verilebilir.

Terim	Tanım
Kripto Süresi	Belirli bir kriptografik anahtarın ,örneğin tanımlanan bir süreyi ve/veya üretilen şifreli metin miktarını esas alarak, ayrıca en iyi sektör uygulamalarına ve kurallarına göre (örneğin, *NIST Özel Yayını 800-57*) tanımlanmış amacına yönelik olarak kullanılabildiği zaman dilimi.
Kriptografi	Bilgi güvenliğiyle, özellikle şifreleme ve kimlik doğrulama ile ilgilenen matematik ve bilgisayar bilimi dalı. Uygulama ve ağ güvenliğinde erişim kontrolü, bilgi gizliliği ve bütünlüğü için kullanılan bir araçtır.
Kriptografik Anahtar Yönetimi	Gerektiğinde eski anahtarları yenileriyle değiştirmek de dâhil olmak üzere, kriptografik anahtarın oluşturulması ve yönetimini destekleyen süreçler ve mekanizmalar bütünü.
Kriptografik Temel	Düz bir metni şifreli metne dönüştürürken bir şifreleme algoritmasının çıktısını belirleyen değer. Anahtarın uzunluğu, genellikle belirli bir mesajda şifreli metni çözme işleminin ne derece zor olacağını belirler. Bkz. *Güçlü Kriptografi.*
Kuruluş	PCI DSS incelemesinden geçen şirketi, organizasyonu veya işletmeyi göstermek için kullanılan terim.
LAN	"Yerel ağ" için kısa ad. Genellikle aynı binada veya bina grubunda ortak bir iletişim hattını paylaşan bilgisayarlar ve/veya diğer cihazlar grubu.
LDAP	"Hafif Dizin Erişimi Protokolü" için kısa ad. Kullanıcı izinlerini sorgulama ve değiştirme ile korumalı kaynaklara erişim için yararlanılan kimlik doğrulama ve yetkilendirme verileri deposu.
LPAR	"Mantıksal bölümleme" için kısaltma. Bir bilgisayarın toplam kaynaklarını (işlemciler, bellek ve depolama) kendilerine ait ayrı işletim sistemi kopyası ve uygulamalarla çalışabilen küçük birimler halinde alt bölümlere ayırma veya bölme sistemi. Mantıksal bölümleme genellikle farklı işletim sistemlerinin ve uygulamaların tek bir cihazda kullanılmasına olanak tanımak için kullanılır. Bölümler, birbiriyle iletişim kurmak veya ağ arayüzleri gibi bazı sunucu kaynaklarını paylaşmak için yapılandırılabilir veya yapılandırılamaz.
MAC	Kriptografide "mesaj kimlik doğrulama kodu" için kısa ad. Bir mesajda kimlik doğrulaması yapmak için kullanılan küçük bir bilgi parçası. Bkz. *Güçlü Kriptografi.*
MAC Adresi	"Ortam erişim kontrolü adresi" için kısaltma. Üreticiler tarafından ağ adaptörlerine ve ağ arayüz kartlarına atanan benzersiz tanımlama değeri.
Manyetik Şerit Verileri	Bkz. *İzleme Verileri.*
Manyetikliğin Bozulması	Ayrıca "disk manyetikliğinin bozulması" olarak da adlandırılır. Diskteki tüm verilerin kalıcı olarak imha edilmesi gibi, diskin manyetikliğini bozan işlem veya teknik.

Terim	Tanım
Maskeleme	PCI DSS bağlamında, bir veri parçasını, görüntülenirken veya yazdırılırken gizleme yöntemidir. Maskeleme, tüm PAN'ı görüntülemeye ilişkin iş gereksinimi olmadığında kullanılır. Maskeleme, görüntülendiğinde veya yazdırıldığında, PAN'ın korunmasıyla ilgilidir. Dosyalarda, veri tabanlarında vb. depolandığında, PAN'ın korunması için bkz. *Kırpılma*.
Misafir Sistem Arakatmanı	Sanal makineleri barındırmaktan ve yönetmekten sorumlu yazılım veya donanım yazılımı. Misafir sistem arakatmanı bileşeni, PCI DSS amaçları doğrultusunda ayrıca sanal makine monitörünü (VMM) de içerir.
MO/TO	“Postayla Sipariş/Telefonla Sipariş" için kısa ad.
MPLS	“Çok Protokollü Etiket Anahtarlaması” için kısa ad. Bir grup paket anahtarlamalı ağı bağlamak için tasarlanan ağ ya da telekomünikasyon mekanizması.
NAC	“Ağ erişim kontrolü" ya da "ağ giriş kontrolü" için kısa ad. Tanımlı bir güvenlik politikasına göre ağ kaynaklarının erişilebilirliğini uç noktası cihazlarıyla kısıtlayarak ağ katmanında güvenlik uygulama yöntemi.
NAT	“Ağ adresi çevirisi” için kısa ad. Ayrıca ağ maskelemesi ya da IP maskelemesi olarak da bilinir. Bir kuruluşun dahili IP adreslerinin içeriden ve harici IP adreslerinin dışarıdan görülmesine izin verecek şekilde, bir ağda kullanılan IP adresini başka bir ağ içinde bilinen farklı bir IP adresi olarak değiştirme.
NIST	“Ulusal Standartlar ve Teknolojiler Enstitüsü” için kısa ad. ABD Ticaret Bakanlığı Teknoloji İdaresi bünyesindeki, düzenleyici olmayan, federal kurum.
NMAP	Ağları eşleyen ve ağ kaynaklarındaki açık bağlantı noktalarını tanımlayan güvenlik tarama yazılımı.
NTP	“Ağ Zaman Protokolü” için kısa ad. Bilgisayar sistemlerinin, ağ cihazlarının ve diğer sistem bileşenlerinin saatlerini eş zamanlı hale getirmek için kullanılan protokol.
NVD	“Ulusal Güvenlik Açığı Veritabanı” için kısa ad. ABD Hükümeti’nin standart tabanlı güvenlik açığı yönetimi verileri deposu. NVD güvenlik kontrol listeleri, güvenlikle ilgili yazılım zafiyetleri, hatalı konfigürasyonlar, ürün adları ve etki ölçümlerine ilişkin veri tabanlarını içerir.
OCTAVE®	“Operasyonel Olarak Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi” için kısa ad. Risk tabanlı bilgi güvenliği stratejisi değerlendirme ve planlama araçları, teknikleri ve yöntemleri.
Organizasyonel Bağımsızlık	Aktiviteyi gerçekleştiren kişi ya da bölümle aktiviteyi değerlendiren kişi ya da bölüm arasında çıkar çatışması olmamasını sağlayan bir organizasyonel yapı. Örneğin, değerlendirmeleri yapan kişiler değerlendirilen ortamın yönetiminden kurumsal olarak ayrıdır.

Terim	Tanım
OWASP	“Open Web Application Security Project (Açık Web Uygulaması Güvenlik Projesi)” için kısa ad. Uygulama yazılımlarının güvenliğini iyileştirmeye odaklanan kâr amacı gütmeyen bir kuruluş. OWASP web uygulamalarına yönelik kritik güvenlik açıkları listesini yönetir. (Bkz. http://www.owasp.org).
Ödeme Kartları	PCI DSS'in amaçları doğrultusunda, üzerinde PCI SSC’nin kurucu üyeleri American Express, Discover Financial Services, JCB International, MasterCard Worldwide veya Visa, Inc.’nin logosunu taşıyan herhangi bir ödeme kartı/ cihazı.
Ödeme Uygulaması	PA-DSS bağlamında, ödeme uygulamasının üçüncü taraflarca satıldığı, dağıtıldığı veya lisanslandığı durumlarda, yetkilendirme veya hesap kapatmanın parçası olarak kart sahibi verilerini kaydeden, işleyen veya yayan bir yazılım uygulaması. Ayrıntılar için bkz. *PA-DSS Program Rehberi*.
Örnekleme	Grubun tamamını temsil eden bir grup kesiti seçme işlemi. Örnekleme, denetçiler tarafından bir kuruluşun standarda, merkezi PCI DSS güvenliğine ve yerleşik operasyonel süreçler ile kontrollere sahip olduğu doğrulandığında genel test eforunu azaltmak için kullanılabilir. Örnekleme bir PCI DSS gerekliliği değildir.
Özel Ağ	Özel IP adresi alanı kullanan bir kuruluş tarafından kurulan ağ. Özel ağlar yaygın biçimde yerel alan ağları gibi tasarlanır. Genel ağlardan özel ağlara erişim güvenlik duvarları ve yönlendiriciler kullanılarak uygun biçimde korunmalıdır.
PA-DSS	“Ödeme Uygulaması Veri Güvenliği Standardı” için kısa ad.
Paket Çözüm	Belirli bir müşteri veya kullanıcı için özel olarak kişiselleştirilmeyen ya da tasarlanmayan, kullanıma hazır, stokta hazır bulunan ürünlerin tanımı.
PAN	“Ana hesap numarası” için kısa ad. Ayrıca “hesap numarası” olarak da anılır. Kart çıkaran kuruluşu ve özel kart sahibi hesabını tanımlayan benzersiz ödeme kartı numarası (genellikle kredi kartları ve banka kartları için).
PA-QSA	“Ödeme Uygulaması Yetkili Güvenlik Denetçisi" için kısa ad. PA-QSA’lar, PCI SSC tarafından ödeme uygulamalarını PA-DSS'e yönelik değerlendirmek için yetkilendirilir. PA-QSA Şirketleri ve Çalışanları için gereksinimler hakkındaki ayrıntılar için bkz. *PA-DSS Program Rehberi* ve *PA-QSA Yeterlilik Gereksinimleri*.
Parametreli Sorgular	Sokuşturma saldırılarından kaçınmak ve bunları engellemek için SQL sorgularını yapılandırmaya yönelik bir araç.
PAT	“Bağlantı noktası adres çevirisi” için kısa ad. Ayrıca “ağ adresi bağlantı noktası çevirisi” olarak da anılır. Aynı zamanda bağlantı noktası numaralarını da çeviren *NAT* türü.
PCI	“Payment Card Industry (Ödeme Kartı Endüstrisi)” için kısa ad.
PCI DSS	“Payment Card Industry (Ödeme Kartı Endüstrisi) Veri Güvenliği Standardı” için kısa ad.

Terim	Tanım
PDA	“Kişisel veri asistanı” ya da “kişisel dijital asistan” için kısa ad. Cep telefonları, e-posta ya da web tarayıcısı gibi özelliklere sahip elde taşınabilen mobil cihazlardır.
PED	PIN giriş cihazı.
Personel	Kuruluşun binasında “yerleşik” veya kart sahibi verileri ortamına farklı şekilde erişebilen tam zamanlı ya da yarı zamanlı çalışanlar, geçici çalışanlar, taşeronlar ve danışmanlar.
PIN	“Kişisel kimlik numarası” için kısa ad. Sistemin kullanıcının kimliğini doğrulaması için yalnızca kullanıcı ve sistem tarafından bilinen gizli sayısal şifre. Kullanıcının erişimine yalnızca kullanıcının girdiği PIN, sistemdeki PIN ile eşleşirse izin verilir. Genel kullanımdaki PIN’ler otomatik para çekme / yatırma makinelerinde nakit avans işlemlerinde kullanılır. Başka bir PIN türü ise, PIN’in kart sahibinin imzası yerine geçtiği çipli EMV kartlarında kullanılan PIN türüdür.
PIN Bloğu	İşlem boyunca PIN’i saklamak için kullanılan veri bloğu. PIN bloğu biçimi, PIN bloğu içeriğini ve PIN'in tekrar elde edilmesi için nasıl işleneceğini tanımlar. PIN bloğu, PIN, PIN uzunluğundan oluşur ve PAN'ın alt kümesini içerebilir.
POI	Verilerin bir karttan okunduğu ilk nokta olan “Etkileşim Noktası” için kısa ad. Elektronik bir işlem kabul ürünü olan POI, donanım ve yazılımdan oluşur ve kart sahibinin işlemi gerçekleştirmesini sağlamak için kabul cihazında yer alır. POI gözetimi altında veya gözetim dışında olabilir. POI işlemleri, genellikle entegre devre (çip) ve/veya manyetik şeritli kart tabanlı ödeme işlemleridir.
Politika	Bilgi işlem kaynaklarının uygun kullanımını, güvenlik uygulamalarını ve operasyonel prosedürlerin geliştirilmesini yöneten organizasyonel kurallar.
POP3	"Posta Ofisi Protokolü Sürüm 3" için kısa ad. E-posta istemcileri tarafından TCP/IP bağlantısı üzerinden uzak sunucudan e-posta almak için kullanılan uygulama katmanı protokolü.
POS	“Satış noktası” için kısa ad. Üye iş yeri lokasyonlarında ödeme kartı işlemlerini gerçekleştirmek için kullanılan donanımlar ve/veya yazılımlar.
Prosedür	Bir politikaya ilişkin tanımlayıcı anlatım şekli. Prosedür, bir politika için “nasıl”ın yanıtıdır ve politikanın nasıl uygulanacağını açıklar.
Protokol	Ağlarda kullanılan, üzerinde anlaşılan iletişim yöntemi. Bilgisayar ürünlerinin bir ağda faaliyet göstermesi için izlemesi gereken kurallar ve prosedürleri tanımlayan spesifikasyonlar.
PTS	“PIN İşlemi Güvenliği” için kısa ad, PTS, PIN kabulü için POI terminallerindeki PCI Security Standards Council tarafından yönetilen modüler bir değerlendirme gereksinimleri bütünüdür. Lütfen bkz. www.pcisecuritystandards.org.
PVV	“PIN doğrulama değeri” için kısa ad. Ödeme kartının manyetik şeridine kodlanan isteğe bağlı değer.

Terim	Tanım
QIR	“Yetkili Entegratör veya Aracı Kurum” için kısa ad. Daha fazla bilgi için PCI SSC web sitesindeki *QIR Program Rehberi*’ne bakın.
QSA	“Yetkili Güvenlik Denetçisi” için kısa ad. QSA'lar PCI SSC tarafından yerinde PCI DSS denetimleri yapmak üzere yetkilendirilir. QSA Şirketleri ve Çalışanları için gereksinimler hakkında ayrıntılar için bkz. *QSA Yeterlilik Gereksinimleri*.
RADIUS	“Remote Authentication Dial-In User Service (Arayan Kullanıcı Kimliğini Uzaktan Doğrulama Hizmeti)” için kısaltma. Kimlik doğrulama ve hesap yönetimi sistemidir. RADIUS sunucusuna iletilen kullanıcı adı ve şifre gibi bilgilerin doğru olup olmadığını kontrol ederek ardından sisteme erişim yetkisi verir. İki öğeli kimlik doğrulama sağlamak için bu kimlik doğrulama yöntemi bir belirteç, akıllı kart vb. ile birlikte kullanılabilir.
Reklam Yazılımı	Kurulduğunda, bilgisayarı otomatik olarak reklamları görüntülemeye veya indirmeye zorlayan kötü niyetli yazılım türü.
RFC 1918	İnternet Mühendisliği Görev Gücü (IETF) tarafından belirlenen, özel (internet yönlendirmesi olmayan) ağların kullanımını ve uygun adres aralıklarını tanımlayan standart.
Risk Analizi / Risk Değerlendirmesi	Değerli sistem kaynaklarını ve bunlara yönelik tehditleri tanımlayan; tahmini olma sıklıklarını ve meydana gelme maliyetlerini esas alarak kayba maruz kalma (kayıp potansiyeli) miktarlarını belirleyen ve (isteğe bağlı olarak) toplam kaybı en aza indirmek için tedbirler öneren süreç.
Risk Sıralaması	Belirli bir kuruluşta yapılan risk değerlendirmesini ve risk analizini esas alan tanımlı bir ölçüm kriteri.
ROC	“Uyum Raporu” için kısa ad. Bir kuruluşun PCI DSS değerlendirmesinden alınan ayrıntılı sonuçları belgeleyen rapor.
ROV	"Geçerlilik Raporu" için kısa ad. PA-DSS programının amaçları doğrultusunda, bir PA-DSS değerlendirmesinden alınan ayrıntılı sonuçları belgeleyen rapor.
RSA	Ortak anahtar şifrelemesi için 1977 yılında Massachusetts Teknoloji Enstitüsü'nde (MIT) Ron Rivest, Adi Shamir ve Len Adleman tarafından tanımlanan algoritma. RSA harfleri soyadlarının baş harflerinden oluşur.
Sanal Anahtar veya Yönlendirici	Sanal anahtar ya da yönlendirici, ağ altyapısı düzeyinde veri yönlendirme ve anahtarlama işlevi sunan mantıksal bir varlıktır. Sanal anahtar, hiper yönetici sürücüsü, modülü ya da eklentisi gibi sanallaştırılmış bir sunucu platformunun ayrılmaz bir parçasıdır.
Sanal Aygıt (VA)	Bir VA belli işlev bütününü yerine getirmek için önceden yapılandırılan bir cihaz kavramını alır ve bu cihazı iş yükü olarak çalıştırır. Genellikle, mevcut bir ağ cihazı, yönlendirici, anahtar veya güvenlik duvarı gibi bir sanal aygıt olarak çalıştırmak üzere sanallaştırılır.
Sanal Hypervisor	Bkz. *Hypervisor*.

Terim	Tanım
Sanal Makine	Ayrı bir bilgisayar gibi hareket eden, bağımsız bir çalışma ortamı. Ayrıca "Konuk" olarak da bilinir ve bir hiper yöneticinin üzerinde çalışır.
Sanal Makine İzleyici (VMM)	VMM, hiper yöneticiye dâhildir ve sanal makine donanım soyutlamasını gerçekleştiren yazılımdır. Her konuk işletim sisteminin ihtiyaç duyduğunu tahsis etmek için sistemin işlemcisini, belleğini ve diğer kaynaklarını yönetir.
Sanal Ödeme Terminali	Sanal ödeme terminali, ticari kuruluşun güvenli olarak bağlanmış bir web tarayıcısı aracılığıyla ödeme kartı verilerini manuel olarak girdiği, ödeme kartı işlemlerini yetkilendirmek için kullanılan kart kabul eden, işleyen veya üçüncü taraf kuruluş web sitesine web tarayıcısı tabanlı bir hizmet sağlayıcı erişimidir. Sanal ödeme terminalleri, fiziksel terminallerden farklı olarak, veriyi doğrudan ödeme kartından okumaz. Ödeme kartı işlemleri manuel olarak girildiğinden, sanal ödeme terminalleri, genellikle düşük işlem hacimli ticari kuruluş ortamlarında fiziksel terminallerin yerine kullanılır.
Sanallaştırma	Sanallaştırma, bilgi işlem kaynaklarının fiziksel kısıtlamalardan mantıksal olarak soyutlanmasıyla ilgilidir. Yaygın bir soyutlama, fiziksel bir makinenin içeriğini alarak farklı fiziksel donanımda ve/veya aynı fiziksel donanımdaki diğer sanal makinelerle birlikte çalışmasını sağlayan sanal makineler ya da VM'ler olarak anılır. Sanallaştırma, VM'lere ek olarak, uygulamalar, masaüstü bilgisayarları, ağlar ve depolama alanları gibi çok sayıda başka bilgi işlem kaynağında gerçekleştirilebilir.
SANS	"Sistem Yöneticisi, Denetim, Ağ İletişimi ve Güvenlik" için kısa ad. Bilgisayar güvenliği eğitimi ve mesleki sertifikalar veren enstitü. (Bkz. www.sans.org.)
SAQ	“Öz Değerlendirme Anketi” için kısa ad. Bir kuruluşun PCI DSS değerlendirmelerinden elde edilen öz değerlendirme sonuçlarını belgelemek için kullanılan raporlama aracı.
SDLC	“Sistem geliştirme yaşam döngüsü" ya da “yazılım geliştirme yaşam döngüsü” için kısa ad. Bir yazılım veya bilgisayar sisteminin planlama, analiz, tasarım, test ve uygulamayı içeren geliştirme aşamaları.
S-FTP	Güvenli FTP için kısa ad. S-FTP kimlik doğrulama bilgilerini ve aktarım halindeki veri dosyalarını şifreleme özelliğine sahiptir. Bkz. *FTP.*
SHA-1/SHA-2	“Güvenli Karma İşlevi Algoritması”. SHA-1 ve SHA-2 dâhil, ilgili kriptografik karma işlevlerinin bir bütünü ya da ailesi. Bkz. *Güçlü Kriptografi.*
Sızma Testi	Sızma testleri, sistem bileşenlerinin güvenlik özelliklerini istismar etmek üzere güvenlik açıklarının suiistimal yöntemlerinin belirlenmesini amaçlar. Sızma testleri, ağ ve uygulama testlerinin yanı sıra ağların ve uygulamaların etrafındaki kontrolleri ve süreçleri içerir. Ayrıca, hem ortam dışında (dış testler) hem de ortam içinde uygulanır.
Sistem Bileşenleri	Kart sahibi verileri ortamında bulunan veya buna bağlanan her türlü ağ cihazı, sunucu, bilgisayar cihazı ya da uygulama.

Terim	Tanım
Sistem düzeyinde nesne	Veritabanı tabloları, kayıtlı prosedürler, uygulamaların yürütülebilen kısımları ile yapılandırma dosyaları, sistem yapılandırma dosyaları, sabit ve paylaşılan kitaplıklar ve DLL'ler, yürütülebilen sistem kısımları, cihaz sürücüleri ve cihaz yapılandırma dosyaları ile üçüncü taraf bileşenleri dâhil, ancak bunlarla sınırlı olmamak kaydıyla bir sistem bileşenindeki, çalışması için gereken her şey.
Siteler Arası İstek Sahteciliği (CSRF)	Kimlik doğrulaması yapılmış bir oturum aracılığıyla istenmeyen eylemlerin yürütülmesini sağlayan, güvenli olmayan kodlama yöntemlerinden kaynaklanan güvenlik açığı. Genellikle XSS ve/veya SQL sokuşturma ile bağlantılı olarak kullanılır.
Siteler Arası Komut Çalıştırma (XSS)	Yanlış giriş geçerlemesine yol açan güvenli olmayan kodlama tekniklerinden oluşan güvenlik açığı. Genellikle CSRF ve/veya “SQL sokuşturma” ile bağlantılı olarak kullanılır.
SNMP	“Basit Ağ Yönetimi Protokolü” için kısa ad. Yönetici ilgisi gerektiren her türlü ağla bağlantılı cihazların izlenmesini destekler.
Sokuşturma Zafiyetleri	Yanlış giriş geçerlemesine yol açan güvenli olmayan kodlama tekniklerinden kaynaklanan güvenlik açığı. Bu güvenlik açığı, saldırganların bir web uygulaması aracılığıyla temeli oluşturan sisteme kötü niyetli kodlar eklemesine izin verir. Bu sınıftaki güvenlik açıkları SQL, LDAP ve XPath sokuşturmalarını içerir.
SQL	“Yapılandırılmış Sorgu Dili” için kısa ad. İlişkisel veritabanı yönetim sistemlerinde veri oluşturmak, değiştirmek ve bunlardan veri almak için kullanılan bilgisayar dili.
SQL Ekleme	Veritabanı odaklı web sitesi saldırısı biçimi. Kötü amaçlı bir kişi internete bağlı bir sistemde güvenli olmayan koddan yararlanarak yetkisiz SQL komutlarını yürütür. SQL ekleme saldırıları, bir veritabanındaki normalde kullanılamayan bilgileri çalmak ve/veya veritabanını barındıran bilgisayar aracılığıyla bir kuruluşun ana bilgisayarlarına erişim sağlamak için kullanılır.
SSH	“Güvenli Kabuk” için kısaltma. Uzaktan oturum açma ya da uzaktan dosya aktarımı gibi ağ hizmetleri için şifreleme sağlayan protokol paketi.
SSL	“Güvenli Yuva Katmanı” için kısa ad. Bir web tarayıcısıyla web sunucusu arasındaki kanalı şifreleyen ve bu kanal üzerinden gönderilen verilerin gizliliğini ve güvenilirliğini sağlayan yerleşik sektör standardı. Bkz. *TLS.*
Sunucu	Diğer bilgisayarlara iletişim kurulması, dosya depolama ya da bir yazıcı olanağına erişim hizmeti sunan bilgisayar. Sunucular, bunlarla sınırlı kalmamak kaydıyla, web, veritabanı, uygulama, kimlik doğrulama, DNS, posta, vekil sunucu ve NTP’yi içerir.
Sürüm Oluşturma Metodolojisi	Bir uygulama ya da yazılımın belirli bir durumunu benzersiz şekilde tanımlamak için sürüm düzenleri atama işlemi. Bu düzenler bir sürüm oluşturma numarasını, sürüm numarası kullanımını ve yazılım satıcısı tarafından tanımlanan herhangi bir joker karakter öğesini takip eder. Sürüm numaraları genellikle artan bir sırada atanır ve yazılımdaki belirli bir değişikliğe karşılık gelir.

Terim	Tanım
Sütun Seviyesinde Veritabanı Şifreleme	Tüm veritabanının bütün içeriği yerine veritabanındaki belirli bir sütunun içeriklerini şifrelemek için kullanılan teknik veya teknoloji (yazılım ya da donanım). Alternatif olarak bkz. *Disk Şifreleme* veya *Dosya Seviyesinde Şifreleme.*
SysAdmin	"Sistem yöneticisi" için kısaltma. Bir bilgisayar sisteminin veya ağının yönetilmesinden sorumlu, yüksek ayrıcalıklara sahip kişi.
Şema	Veri öğelerinin düzenlenmesi dâhil olmak üzere bir veritabanının yapılandırılma şeklinin resmi tanımı.
Şifre / Parola	Kullanıcının kimliğini doğrulamak için kullanılan karakter dizisi.
Şifre Kırma Tablosu Saldırısı	Genellikle şifreleri veya kart sahibi veri karmalarını kırmak için orijinal veri kaynağını belirlemek üzere önceden hesaplanan bir karma işlevi dizesi tablosu (değişmeyen uzunlukta mesaj özeti) kullanılan veri saldırısı yöntemi.
Şifreleme	Bilgileri, belirli bir kriptografik anahtarı olan kişiler dışındakiler için anlaşılmaz bir biçime dönüştürme işlemi. Şifrelemenin kullanılması, şifreleme işlemi ve şifre çözme işlemi arasında (şifrelemenin tersi) bilgileri yetkisiz ifşaya karşı korur. Bkz. *Güçlü Kriptografi.*
Şifreleme Algoritması	Ayrıca "kriptografik algoritma" olarak da adlandırılır. Şifrelenmemiş bir metnin veya verinin, şifrelenmiş metne veya veriye dönüştürülmesi ve tekrar eski haline çevrilmesi için kullanılan matematiksel talimatlar dizisi. Bkz. *Güçlü Kriptografi.*
TACACS	"Terminal Erişimi Kontrol Birimi Erişimi Kontrol Sistemi" için kısa ad. Çoğunlukla bir uzaktan erişim sunucusu ile bir kimlik doğrulama sunucusu arasında iletişim kuran ağlarda ağa kullanıcı erişimi haklarını belirlemek için kullanılan uzaktan kimlik doğrulama protokolü. İki öğeli kimlik doğrulama sağlamak için bu kimlik doğrulama yöntemi bir belirteç, akıllı kart vb. ile birlikte kullanılabilir.
Tampon Taşması	Bir programın arabelleğin sınırını aştığı ve verileri bitişik bellek alanına yazdığı durumlarda, güvenli olmayan kodlama yöntemlerinin oluşturduğu güvenlik açığı. Tampon taşmaları saldırganların sistemlere veya verilere izinsiz erişiminde kullanılır.
Taşınabilen Elektronik Medya	Dijital hale getirilmiş verileri depolayan, kolayca kaldırılabilen ve/veya bir bilgisayar sisteminden diğerine taşınmasını sağlayan ortam. Taşınabilen elektronik ortamlara CD-ROM, DVD-ROM, USB flaş bellekler ve taşınabilen sabit sürücüler verilebilir.
TCP	"İletim Denetimi Protokolü" için kısa ad. İnternet Protokolü (IP) paketinin temel taşıma katmanı protokollerinden biri ve temel iletişim dili ya da internetin protokolü. Bkz. *IP*.
TDES	"Üçlü Veri Şifreleme Standardı" için kısaltma. Ayrıca "3DES" ya da "Üçlü DES" olarak da bilinir. DES şifrelemeden üç kez kullanılarak oluşturulan blok şifreleme. Bkz. *Güçlü Kriptografi.*

Terim	Tanım
Tehdit	Bilgi ya da bilgi işleme kaynaklarının kasten veya kazara kaybolmasına, değiştirilmesine, açığa çıkmasına, erişilemez hale gelmesine veya başka şekilde kuruluşun zarar görmesine neden olma olasılığı bulunan koşul veya faaliyet.
Telafi Edici Kontroller	Telafi edici kontroller, makul teknik veya belgeye dayalı iş kısıtları nedeniyle, bir kuruluşun bir gereksinimi ifade edildiği gibi karşılayamadığı, ancak diğer kontrollerin uygulanması aracılığıyla gereksinimle ilgili riskin makul seviyede azaltıldığı durumlar olarak değerlendirilebilir. Telafi edici kontroller: (1) Orijinal PCI DSS gereksiniminin amacını ve koşullarını karşılamalıdır; (2) Orijinal PCI DSS gerekliliğiyle benzer bir koruma düzeyi sağlamalıdır; (3) Diğer PCI DSS gereksinimlerinin (yalnızca diğer PCI DSS gereksinimleriyle uyum içinde değil) ötesinde olmalıdır ve (4) PCI DSS gerekliliğine uymama sonucu ortaya çıkan ek riskle orantılı olmalıdır. Telafi edici kontrollerin kullanımıyla ilgili rehberlik için *PCI DSS Gereksinimleri ve Güvenlik Değerlendirmesi Prosedürleri* bölümündeki "Telafi Edici Kontroller" Ek B ve CÜ'ye bakın.
TELNET	"Telefon şebekesi protokolü" için kısaltma. Genellikle bir ağdaki cihazlarda kullanıcı odaklı komut satırı giriş oturumları sağlamak için kullanılır. Kullanıcı bilgileri düz metin biçiminde iletilir.
Ticari Kuruluş	PCI DSS'nin amaçları doğrultusunda, bir ticari kuruluş, mallar ve/veya hizmetler için ödeme olarak PCI SSC'nin beş üyesinden herhangi birinin (American Express, Discover, JCB, MasterCard ya da Visa) logosunu taşıyan ödeme kartlarını kabul eden her türlü kuruluş olarak tanımlanır. Mal ve/veya hizmetler karşılığında ödeme olarak ödeme kartlarını kabul eden bir ticari kuruluşun, satılan hizmetler diğer satıcılar veya hizmet sağlayıcılar adına kart sahibi verilerinin depolanmasıyla, işlenmesiyle ya da yayılmasıyla sonuçlanırsa bir hizmet sağlayıcı olabileceğini de unutmayın. Örneğin, bir ISP, aylık faturalar için ödeme kartlarını kabul eden bir ticari kuruluştur, ancak ticari kuruluşlara müşterileri olarak hizmet veriyorsa aynı zamanda bir hizmet sağlayıcıdır.
TLS	"Aktarım Katmanı Güvenliği" için kısa ad. İletişim halindeki iki uygulama arasında veri gizliliği ve veri bütünlüğü sağlama amacıyla tasarlanmıştır. TLS, SSL'nin ardılıdır.
Truva	Ayrıca "Truva atı" olarak da anılır. Kurulduğunda, bir yandan kullanıcının normal işlerini yapmasını sağlarken, diğer yandan kullanıcının bilgisi olmadan bilgisayar sisteminde kötü amaçlı işlevler gören bir kötü amaçlı yazılım türü.
Tüketici	Mal, hizmet veya ikisini birden satın alan kişi.
Tüketici Olmayan Kullanıcılar	Çalışanlar, yöneticiler ve üçüncü taraflar dâhil, ancak bunlarla sınırlı olmamak kaydıyla, sistem bileşenlerine erişen, kart sahipleri dışındaki kişiler.

Terim	Tanım
URL	“Uniform Resource Locator (Tekdüzen Kaynak Konum Belirleyicisi)" için kısa ad.Web tarayıcıları, e-posta istemcileri ve diğer yazılımlar tarafından internette bir ağ kaynağını tanımlamak için kullanılan biçimlendirilmiş metin dizesi.
Uygulama	Hem dâhili hem de harici uygulamalar (örneğin, web) olmak üzere tüm satın alınan ve kuruma göre uyarlanmış nitelikteki yazılım programlarını veya program gruplarını içerir.
Uzak Laboratuvar Ortamı	PA-QSA tarafından yönetilmeyen bir laboratuvar.
Uzaktan Erişim	Bilgisayar ağlarına uzak bir lokasyondan erişim. Uzaktan erişim bağlantıları, şirketin kendi ağının içinden ya da şirket ağının dışındaki uzak bir yerden başlayabilir. Uzaktan erişim teknolojisinin bir örneği *VPN*'dir.
Varsayılan Hesaplar	Bir sistemde, uygulamada veya cihazda, sistem ilk kez hizmete alındığında ilk erişimi sağlamak için önceden tanımlanan giriş hesabı. Kurulum işleminin bir parçası olarak sistem tarafından ek varsayılan hesaplar oluşturulabilir.
Varsayılan Şifre	Genellikle varsayılan hesapla ilişkili bir sistemde, uygulamada veya cihazda önceden tanımlanan sistem yönetimi, kullanıcı veya hizmet hesabıyla ilgili şifre. Varsayılan hesaplar ve şifreler yayınlanmış ve iyi bilinir olduklarından, kolayca tahmin edilebilir.
Vekil Sunucu	Dâhili bir ağ ile internet arasında aracı olarak görev yapan bir sunucu. Örneğin, bir vekil sunucunun işlevlerinden biri, dâhili ve hârici bağlantılar arasındaki bağlantıları, her biri yalnızca vekil sunucuyla iletişim kuracak şekilde sonlandırmak veya uzlaştırmaktır.
Veri Akışı Şeması	Verilerin bir uygulama, sistem veya ağ boyunca nasıl aktığını gösteren şema.
Veritabanı	Kolayca geri getirilebilen bilgileri düzenlemek ve yönetmek için yapılandırılmış format. Basit veritabanı örnekleri, tablolar ve elektronik çizelgelerdir.
Veritabanı Yöneticisi	Ayrıca “DBA” olarak da anılır. Veri tabanlarının yönetiminden ve idaresinden sorumlu kişi.
Virüsten Koruma	Virüsler, solucanlar, Truvalar veya Truva atları, casus yazılımlar, reklam yazılımları ve kök kullanıcı takımı(işletim sisteminde arka planda çalışan gizli programlar) gibi çeşitli kötü niyetli yazılımları (“kötücül yazılım” da denir) belirleyebilen, kaldırabilen ve bunlara karşı koruma sağlayabilen program veya yazılım.
VLAN	“Sanal LAN” ya da “sanal yerel ağ” için kısaltma. Tek bir geleneksel fiziksel yerel ağın ötesine uzanan mantıksal yerel ağ.

Terim	Tanım
VPN	"Sanal özel ağ" için kısa ad. Fiziksel kablolarla doğrudan bağlantılar yerine internet gibi bazı büyük ağlar dahilinde bağlantıların bazıları sanal devreler olan bir bilgisayar ağı. Durum bu olduğunda sanal ağın uç noktasının, büyük ağ aracılığıyla tünellendiği ifade edilir. Yaygın bir uygulama genel internet boyunca güvenli iletişimden oluşurken, bir VPN, kimlik doğrulama ya da içerik şifrelemesi gibi güçlü güvenlik özelliklerine sahip olabilir ya da olmayabilir. VPN, çift öğeli kimlik doğrulama sağlamak için bir belirteç, akıllı kart vb. ile birlikte kullanılabilir.
WAN	"Geniş alan ağı" için kısa ad. Genellikle bölgesel veya şirket çapında olmak üzere geniş bir alanı kapsayan bilgisayar ağı.
Web Sunucusu	Web istemcilerinden gelen HTTP isteklerini kabul eden ve HTTP yanıtlarını (genellikle web sayfaları) gönderen bir program içeren bilgisayar.
Web Uygulaması	Genellikle bir web tarayıcısı ya da web hizmetleri aracılığıyla erişilen bir uygulama. Web uygulamaları internet ya da özel, dâhili bir ağ üzerinden kullanılabilir.
WEP	"Kablolu Eşdeğer Mahremiyet" için kısa ad. Kablosuz ağları şifrelemek için kullanılan zayıf algoritma. Sektör uzmanları tarafından, bir WEP bağlantısının dakikalar içinde hazır yazılımla kırılabileceği gibi bazı ciddi zayıf yönler belirlenmiştir. Bkz. *WPA.*
WLAN	"Kablosuz yerel ağ" için kısa ad. İki ya da daha fazla bilgisayarı veya cihazı kablosuz olarak bağlayan yerel ağ.
WPA/WPA2	"WiFi Korumalı Erişim" için kısa ad. Kablosuz ağları güvenlik altına almak için oluşturulan güvenlik protokolü. WPA, WEP'nin ardılıdır. WPA2 de aynı zamanda WPA'nın gelecek nesli olarak kullanıma sunulmuştur.
Yama	Mevcut yazılıma yeni bir işlev eklemek ya da bir kusuru düzeltmek için yapılan güncelleme.
Yedekleme	Arşivleme ya da hasar veya kaybolmaya karşı koruma amacıyla, verilerin iki kopya halinde çoğaltılması.
Yeniden Anahtar Oluşturma	Kriptografik anahtarları değiştirme işlemi. Periyodik yeniden anahtar oluşturma işlemi, tek bir anahtar tarafından şifrelenen veri miktarını sınırlandırır.
Yetkilendirme	Erişim kontrolü bağlamında, yetkilendirme bir kullanıcıya, programa veya işleme erişim hakkı veya diğer hakları vermektir. Yetkilendirme, başarılı kimlik doğrulamadan sonra bir kişinin veya programın yapabileceklerini tanımlar. Ödeme kartı işlemleri bağlamında, yetkilendirme kart kabul eden kuruluş, kart çıkaran/işlemci kuruluşla işlemi doğruladıktan sonra üye iş yeri işlem onayı aldığında gerçekleşir.

Terim	Tanım
Yönlendirici	İki ya da daha fazla ağı bağlayan donanımlar ya da yazılımlar. Adreslere bakarak ve bilgi parçacıklarını uygun varış yerlerine ileterek bir sıralayıcı ve yorumlayıcı olarak görev yapar. Yazılım yönlendiricileri zaman zaman “ağ geçidi” olarak anılır.