White Paper

pitney bowes

Postbearbeitung und Versand
Verwaltung eingehender Sendungen

Maximieren Sie Ihre Datensicherheit.

SendSuite Tracking Online ist eine SaaS-basierte Lösung von Pitney Bowes, die die Protokollierung, Nachverfolgung und Verwaltung von eingehenden Paketen und Briefen optimiert. Mit dieser Lösung erhalten Sie eine bessere Übersicht über alle Sendungen, die in Ihrem Unternehmen eingehen sowie über deren Bestimmungsort. Dadurch profitieren Sie von präziseren und effizienteren Prozessen.

SendSuite Tracking Online ist eine professionelle Lösung, die einen hohen Grad an Informationssicherheit und Datenschutz bietet. Die Lösung ist als gehostete Unternehmensanwendung verfügbar. Immer mehr Unternehmen verwenden gehostete Software anstelle von On-Premise-Software. Pitney Bowes bietet diese Anwendung als gehostete Software, um:

- die Bereitstellung der Lösung zu erleichtern;
- IT-Ressourcen der Kunden freizustellen, damit diese sich auf ihre wichtigsten Geschäftstätigkeiten konzentrieren können;
- für eine problemlose Softwareimplementierung zu sorgen.

Ziele des White Papers

- Sie verstehen die Vorteile unserer Hostinglösung.
- Sie erhalten eine umfassende Einführung in die Sicherheits- und Datenschutzfunktionen von SendSuite Tracking Online.
- Sie erhalten eine Übersicht über die Verwaltungs- und Überwachungskomponenten dieser Hostinglösung.

Warum sollten Sie sich für eine Hostinglösung von Pitney Bowes entscheiden?

SendSuite Tracking Online bietet Ihnen einen unternehmerischen Vorteil. Dieser wird durch die Reduzierung interner IT-Ressourcen und Kosteneinsparungen zur Einhaltung von Budgetbeschränkungen noch weiter verstärkt.

- Möglicherweise ist die Auslagerung von Anwendungen oder die Nutzung von SaaS-Angeboten (Software as a Service) in den Unternehmensrichtlinien festgelegt.
- Infolge von Einschränkungen durch die Firewall des Unternehmens und/oder aufgrund anderer Sicherheitsaspekte ist ein externes Hosting die bevorzugte Lösung.

Sicherheitsarchitektur

Die Sicherheitsarchitektur von SendSuite Tracking Online umfasst sowohl das Design als auch die Wartung der sicheren Plattform. Sie wurde zum Schutz der Daten von Direktkunden und grundsätzlich zum Schutz aller Daten entwickelt. Sämtliche Anwendungsfunktionen sind so ausgerichtet, dass sie den strengen Sicherheits- und Datenschutzrichtlinien von Pitney Bowes entsprechen.

SendSuite Tracking Online wird auf speziellen Instanzen von Amazon Web Services (AWS) bereitgestellt. Es umfasst Verschlüsselung im Transit und Ruhezustand über EBS-Volume-Verschlüsselung sowie SSL-Kommunikation zwischen Anwendungsservern und der Datenbank. SSL-Zertifikate werden auf dem Load Balancer Layer von Amazon bereitgestellt, und alle Protokolle werden unter Einhaltung der Datenschutzrichtlinie von Pitney Bowes gespeichert. Die Anwendungsserver verfügen über gesicherte Betriebssysteme, um potenzielle Schwachstellen zu beseitigen.

Plattformsicherheit

Sicherheit und Zugriff auf die Hostingeinrichtung

Die Lösung SendSuite Tracking Online von Pitney Bowes wird in erstklassigen Hostingeinrichtungen bereitgestellt. Diese Einrichtungen werden von Amazon Web Services (AWS) verwaltet und befinden sich für die internationale und europäische Implementierung in Irland.

Die von AWS bereitgestellte IT-Infrastruktur wurde bzw. wird nach Best Practices im Bereich Sicherheit konzipiert. Die AWS-IT-Infrastruktur verwaltet und erfüllt die Anforderungen verschiedener IT-Sicherheitsstandards, einschließlich:

- SOC 1/SSAE 16/SAE 3402
- SOC 2
- SOC 3
- FISMA, DIACAP und FedRAMP
- PCI DSS Level 1
- ISO 27001
- ISO 9001
- ITAR
- FIPS 140-2

AWS bietet extrem sichere Datenzentren an, die modernste elektronische und Multifaktor-Steuerungssysteme verwenden, einschließlich:

- Eines hochsicheren Produktionsgebäudes mit Rund-um-die-Uhr-Bewachung, geschlossenem Schaltkreis, alarmgeschützten Türen mit gesichertem Zugang durch Schlüsselkarten, biometrischem Scanner und eingeschränktem Zugang zum Stockwerk, in dem sich Daten befinden.
- Eines fortlaufend überwachten Gebäude- und Umgebungskontrollsystems.

Netzwerkschutz

Außerdem werden zum Schutz vor unbefugten Zugriffen verschiedene Maßnahmen ergriffen:

- Redundante, fehlertolerante Firewalls zur Segmentierung und zum Schutz des Datenverkehrs
- SSL-Zertifikat (HTTPS)
- Services der Präsentationsschicht werden ausschließlich in der DMZ abgelegt.

Beurteilung vor der Installation

Alle Systeme werden vor der Aufnahme in die Produktion einer sorgfältigen Beurteilung hinsichtlich ihrer Sicherheit und möglicher Schwachstellen unterzogen. Gegebenenfalls kann eine Zusammenfassung der Sicherheitsbeurteilung der Anwendung bereitgestellt werden.

Gemeinsame Verantwortung für die Bereitstellung der Anwendung in AWS

Verantwortlichkeiten von AWS:

01. Netzwerksicherheit
02. Sicherheit des Rechenzentrums
03. Ermöglichen von Notfallwiederherstellung und Kontinuitätsplanung

Anwendungsbezogene Verantwortlichkeiten von Pitney Bowes:

01. Vulnerability Scan der Anwendung
02. Penetrationstest der Anwendung
03. Sicherheitsüberprüfungen der bereitgestellten AWS-Infrastruktur
04. Statische Codeanalyse des Anwendungscodes

Für weitere Informationen zu SendSuite Tracking Online wenden Sie sich bitte an Ihren technischen Berater bei Pitney Bowes.

Anwendungssicherheit

Pitney Bowes integriert die erforderlichen Sicherheitsmaßnahmen in jeden einzelnen Prozessschritt der Plattformentwicklung. Vom Softwaredesign über die Software- und Hostingarchitektur bis hin zum Support nach dem Software-Release werden Sicherheitserwägungen immer einbezogen.

Die Anforderungen von SendSuite Tracking Online entsprechen den ENISA- und FFIEC-Richtlinien. Diese Richtlinien wurden in den Produktentwicklungs- und Bereitstellungsanforderungen umgesetzt.

Sicherheitsarchitektur und -design wurden überprüft, um sicherzugehen, dass die Sicherheitskontrollen unter Berücksichtigung dieser technischen Daten auf das System angewandt wurden. Diese Kontrollen werden sowohl auf Daten im Transit als auch auf Daten im Ruhezustand angewandt.

Kontinuierliche Tests

Regelmäßige Penetrationstests
Penetrationstests werden einmal im Jahr von Dritten ausgeführt, um sicherzustellen, dass mögliche Sicherheitsschwachstellen behoben werden. Alle Eingabe- und Ausgabepfade werden mit Fokus auf Datensicherheit ausgeführt.

Laufende Bewertung der Betriebssystemsicherheit
Alle Systeme werden routinemäßig gescannt, um Viren und andere Bedrohungen zu erkennen und entsprechende Schutzmaßnahmen zu ergreifen. Zudem werden wichtige Aktualisierungen des Betriebssystems ausgeführt, um sicherzustellen, dass es auch vor den neuesten Sicherheitsschwachstellen geschützt ist.

Schwachstellen werden mithilfe automatischer Bereitstellungen und Aktualisierungen in der gesamten Cloud-Infrastruktur und in der gesamten Umgebung ausgebessert. Dazu gehören:

- Konnektivität
- Betriebliches Kontinuitätsmanagement
- Geschäftslogik
- Upgrade-Strategie

Verteidigung
Pitney Bowes richtet sich nach den branchenüblichen Best Practices für Softwaresicherheit. Bei Pitney Bowes sind alle Computer durch eine Viruserkennungssoftware auf Unternehmensebene geschützt. Im Folgenden werden einige bewährte Verfahren von Pitney Bowes bei der Entwicklung von Softwarelösungen aufgeführt:

- Austausch vertraulicher Daten mit den Servern per TLS
- Schulungen zum Thema Sicherheitsbewusstsein für Softwareentwickler
- Automatisierte Penetrationstests und Codeanalysen
- Entwurfs- und Begutachtungsverfahren mit Code-Prüfung
- Ethical-Hacker-Schulungen
- Digital signierte Software

HTTPS und sicheres FTP
Pitney Bowes bietet HTTPS für die sichere Übertragung von Dateien an Ihre Kunden bzw. von Ihren Kunden an unser Zentrum für gehostete Daten.

Mitarbeitersicherheit

Authentifizierung

Als Authentifizierungsmethode speichert SendSuite Tracking Online die Benutzer-IDs in der Anwendungsdatenbank und gleicht sie mit dem Pitney Bowes kundenspezifischen „Mein Konto" ab. Kennwörter werden nicht in Klartext übertragen oder gespeichert.

Serverstatus- und Sicherheitsüberwachung

CPU-Nutzung, verfügbarer Festplattenspeicher, Fehler bei Hardwarekomponenten, Netzwerkverfügbarkeit, Anwendungsverfügbarkeit usw. werden mithilfe der verschiedenen nachfolgend beschriebenen Tools fortlaufend überwacht. SendSuite Tracking Online erfasst mittels konsolidierter Protokollierung und Analysen Sicherheitsanomalien und benachrichtigt gegebenenfalls das Support-Team in Echtzeit.

Amazon CloudWatch
Mit der Amazon CloudWatch können die wichtigsten Metriken auf Server-Ebene überprüft werden. Sobald eines der Attribute einen vordefinierten Schwellenwert überschreitet, werden Warnungen erstellt, die Tickets zur Problembehebung generieren. Diese Tickets werden vom Network Operations Center bearbeitet. Dort wird das Problem identifiziert und sortiert (siehe Abschnitt „Warnungen"). Die Performance-Attribute, die auf Server-Ebene durch die CloudWatch Services überwacht werden, beinhalten:

- CPU
- Arbeitsspeicher
- Netzwerkbandbreite

AppDynamics
AppDynamics wird verwendet, um die Leistung der verschiedenen Lösungskomponenten zu überwachen. So werden unsere Support-Mitarbeiter frühzeitig vor möglichen Problemen gewarnt. Sie werden benachrichtigt, wenn Transaktionen zwischen verschiedenen Ebenen keine Baseline-konforme Leistung erbringen. Sobald die festgelegten Schwellenwerte überschritten werden, werden Warnungen erstellt, die wiederum Tickets zur Problembehebung generieren. Diese Tickets werden an das Network Operations Center übermittelt. Dort wird das Problem identifiziert und sortiert (siehe nachfolgender Abschnitt „Warnmeldungen").

Keynote
Keynote wird für die Überwachung der Benutzererfahrung mit SendSuite Tracking Online eingesetzt. Diese erfolgt durch die Ausführung synthetischer Transaktionen mit der Dienstleistung von mehreren Standorten auf der ganzen Welt (Hinweis: So werden falsche Alarme aufgrund lokaler Netzwerkprobleme bei einem einzelnen Keynote-Überwachungsstandort vermieden).

Mithilfe von Keynote wird die Baseline der Lösungsperformance bei normalem Betrieb festgelegt und eine Warnung ausgelöst, wenn der Schwellenwert überschritten wird. Mit Keynote kann Pitney Bowes zudem von einer unabhängigen Quelle Berichte zur Leistung der Anwendung im Vergleich zu den SLAs bereitstellen.

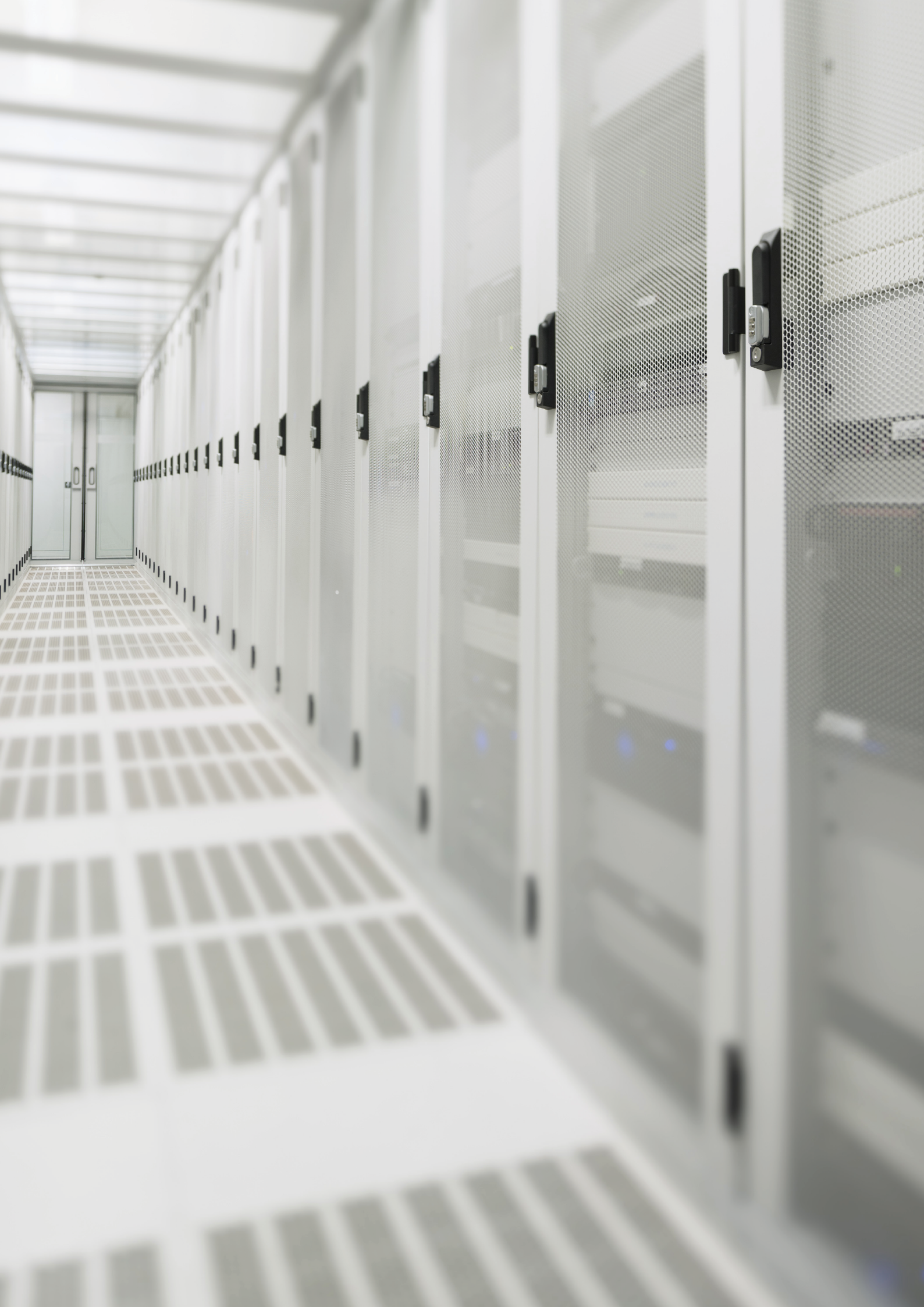
Warnmeldungen
Warnmeldungen werden automatisch im Issue Tracking System von Pitney Bowes protokolliert. Je nach Schweregrad der Warnmeldung werden automatisch die entsprechenden primär zuständigen Personen benachrichtigt. Jeder gehosteten Pitney Bowes-Anwendung wird ein Notfall-Team (ERT) zugeteilt, das je nach Schweregrad der Warnung durch ein spezielles Telefonkonferenzsystem einberufen werden kann. Die Notfallteams bestehen aus Projektmanagern, Anwendungstechnikern, Hardware-, Netzwerk- und Datenbankadministratoren und IT-Managern.

Verschiedene Gruppen können Warnungen empfangen und Probleme identifizieren, z. B. in den folgenden Bereichen:
- Team Softwareimplementierung
- Team Operations
- Call Center Team
- Kunde

Die Lösung generiert verschiedene Arten von Warnungen. Sie reichen von Infrastruktur über Anwendung bis hin zu Sicherheit.

Zusammenfassung:
Mit SendSuite Tracking Online können Benutzer ihre Prozesse für eingehende Sendungen und Anlagenverläufe optimieren und verbessern. Pitney Bowes bietet Hosting an, um seinen Kunden eine vereinfachte Implementierung sowie die Freistellung gebundener IT-Ressourcen zu ermöglichen, damit diese sich auf ihre wichtigsten Geschäftstätigkeiten konzentrieren können.

Für weitere Informationen zu SendSuite Tracking Online wenden Sie sich bitte an Ihren technischen Berater bei Pitney Bowes.



Glossar

AWS Amazon Web Services.

CPU Central Processing Unit (Hauptprozessor).

DIACAP Department of Defense Information Assurance Certification and Accreditation Process (etwa: Maßnahmen des US-Verteidigungsministeriums für die Zertifizierung und Akkreditierung von Informationssicherheit)

DMZ Demilitarized Zone (Entmilitarisierte Zone)

ENISA Agentur der Europäischen Union für Netz- und Informationssicherheit, ursprünglich Europäische Agentur für Netz- und Informationssicherheit

ERT Emergency Response Team (Notfallteam)

FedRAMP Federal Risk and Authorization Management Program (ein Genehmigungsprogramm der US-Regierung)

FFIEC Federal Financial Institutions Examination Council (US-amerikanische Bundesbehörde zur Prüfung von Finanzinstituten)

FIPS 140-2 Der Federal Information Processing Standard (FIPS) Publication 140-2 ist eine Computersicherheitsnorm der US-Regierung zur Zertifizierung kryptographischer Module.

FISMA Federal Information Security Management Act (etwa: US-Bundesgesetz zur Sicherheit von Informationsdaten)

FTP File Transfer Protocol (Netzwerkprotokoll zur Dateiübertragung)

ID Kennung.

ISO 9001 Ein zertifiziertes Qualitätsmanagementsystem für Unternehmen, die nachweisen wollen, dass sie konsistent Produkte und Dienstleistungen anbieten, die auf die Bedürfnisse der Kunden und andere Stakeholder zugeschnitten sind.

ITAR International Traffic in Arms Regulations (etwa: internationale Regelungen zum Waffenhandel)

IT Informationstechnologie

OS Operating System (Betriebssystem)

OWASP Open Web Application Security Project (etwa: Projekt zur Sicherheit in offenen Web-Anwendungen)

PB Pitney Bowes

PCI DSS Level 1 Payment Card Industry Data Security Standard (etwa: der Industrienorm entsprechender Standard für Zahlungskarten)

(I)SAE 3402 (International) Standard on Assurance Engagements (etwa: (internationaler) Standard im Hinblick auf Prüfungsaufträge)

SLA Service Level Agreement

SOC 1 (Service Organization Control 1) Ein Bericht über interne Kontrollmechanismen bei Dienstleistungsunternehmen, die für die Überprüfung der Finanzberichterstattung eines Benutzers relevant sind.

SOC 2 Dieser Bericht enthält Informationen zu den Kontrollmechanismen eines Unternehmens im Hinblick auf nicht-finanzielle Aspekte. Er bezieht sich auf Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz eines Systems.

SOC 3 Dieser Bericht enthält allgemeine Informationen zum Prüfbericht sowie Informationen, ob das System die Kriterien des Dienstleistungsvertrauens erfüllt hat.

SSAE 16 Statement on Standards for Attestation Engagements (etwa: Bericht über Standards im Hinblick auf Prüfungsaufträge) Nr. 16, Bericht über Kontrollmechanismen bei Dienstleistungsunternehmen.

SSL Secure Sockets Layer ist eine standardisierte Sicherheitstechnologie zur Herstellung einer verschlüsselten Verbindung zwischen einem Webserver und einem Browser (sicher).

Pitney Bowes Deutschland GmbH
Poststraße 4-6
64293 Darmstadt
06151 5202 0
contact.de@pb.com

Weitere Informationen erhalten Sie unter der Telefonnummer 06151 5202 0
oder auf unserer Website pitneybowes.com/de.

16ECM08506_DE