

Externer PCI DSS Security Scan (ASV Scan)

Requirement 11.2.2



Zum Nachweis der PCI DSS Compliance müssen Unternehmen, die Kreditkartendaten verarbeiten, speichern oder weiterleiten, ihre IT-Systeme quartalsweise mit einem externen Scan auf Schwachstellen überprüfen.

Mit den ASV Scans der usd erfüllen Sie das PCI DSS Requirement 11.2.2 (quarterly external vulnerability scans). Auf unserer usd PCI DSS Plattform erhalten Sie nach der erfolgreichen Durchführung die Attestation of Scan Compliance sowie einen detaillierten technischen und managementtauglichen Bericht.

Was kennzeichnet unseren Scan?

Seit 2005 ist die usd durch das PCI Security Standards Council (PCI SSC) autorisiert, Sicherheitsprüfungen gemäß des Standards PCI DSS durchzuführen. Als Approved Scanning Vendor (ASV) führen wir bei unseren Kunden weltweit ASV Scans durch. Sie erhalten bei PCI relevanten Findings eine unbegrenzte Anzahl kostenfreier Re-Scans - bis Ihr Scanergebnis PCI DSS compliant ist. Unser mehrsprachiges PCI Competence Center unterstützt Sie gezielt und kompetent bei Rückfragen.



The PCI Security Standards Approved Scanning Vendor logo is a trademark or service mark of The PCI Security Standards Council in the United States and in other countries.

Preise

Einmal-Scan	Jahrespaket
für 1 IP-Adresse 220,- Euro*	4 Scans für 1 IP-Adresse 780,- Euro*
+	+
für jede weitere IP-Adresse 12,- Euro*	4 Scans für jede weitere IP-Adresse 39,- Euro*
Unbegrenzte Re-Scans bei PCI relevanten Findings bis der PCI DSS compliant-Status erreicht ist. kostenlos	Unbegrenzte Re-Scans bei PCI relevanten Findings bis der PCI DSS compliant-Status erreicht ist. kostenlos

*Alle Preise verstehen sich zzgl. der gesetzlich geltenden MwSt.

Gerne vereinbaren wir mit Ihnen auch individuelle Preismodelle. Bitte sprechen Sie uns hierzu einfach an.

Ihr Scanablauf



Registrierung

Registrieren Sie sich auf der usd PCI DSS Plattform und wählen Sie den Zeitpunkt sowie die Ziele Ihres Scans. Infos finden Sie unter:

<https://pci.usd.de/>



Planung

Die ASV Scans werden je IP-Adresse durchgeführt. Sollten Sie nicht sicher sein, welche IP-Adressen gemäß PCI DSS in Scope sind, helfen Ihnen unsere Experten des PCI Competence Centers gerne weiter.



Scan

Wir überprüfen mit einem normierten, international anerkannten Verfahren Ihre aus dem Internet erreichbaren IT-Systeme. Erkannte Schwachstellen werden nicht ausgenutzt. Eine Gefährdung des ordnungsgemäßen Betriebs Ihrer IT-Systeme ist nahezu ausgeschlossen.



Review

Einer unserer Approved Scanning Vendor Professionals führt einen Review Ihres Scanergebnisses durch. Er bewertet Findings hinsichtlich der PCI DSS Compliance und trifft Maßnahmenempfehlungen für Sie. Im Anschluss haben Sie die Möglichkeit, Findings zu kommentieren und False Positives zu melden.



Bericht

Sie erhalten einen umfassenden Bericht bestehend aus einer Executive Summary und einem Technical Report. Darüber hinaus erhalten Sie die Attestation of Scan Compliance, die für den Nachweis Ihrer PCI DSS Compliance erforderlich ist. Kritikalität von Findings und Eintrittsrisiken werden bewertet sowie Maßnahmenempfehlungen darin gegeben.



Siegel & Zertifikat

Sofern Ihr Scanergebnis PCI DSS compliant ist und Sie gemäß den PCI DSS Vorgaben Ihren SAQ ausgefüllt bzw. erfolgreich ein Onsite Audit durchlaufen haben, erhalten Sie Ihr PCI DSS Compliance Siegel und Zertifikat.

Dieses Produktblatt hat Gültigkeit, sofern keine aktuellere Version veröffentlicht wurde. *Erstellungsdatum Produktblatt: 05.07.2019*

Pflichten, Haftung, Allgemeines

Für die mit diesem Vertrag vereinbarte Sicherheitsanalyse gelten nachfolgend beschriebene Regelungen.

Stornierung, Ausfallhonorar

Bei Stornierung von Terminen durch den Auftraggeber zahlt dieser für Absagen mit einer kürzeren Vorlaufzeit als fünf Werktage vor Durchführungstermin 100% des vereinbarten Honorars als Ausfallhonorar, sofern der Auftragnehmer den durch die Terminabsage freigegebenen Zeitraum nicht anderweitig wirtschaftlich einsetzen kann. Gleiches gilt für den Fall einer kurzfristigen Terminverschiebung durch den Auftraggeber. Absagen oder Terminverschiebungen müssen stets schriftlich per E-Mail, Fax oder Brief erfolgen.

Mitwirkungspflichten des Auftraggebers

Mit Unterzeichnung dieses Angebots versichert der Auftraggeber, dass die technische Sicherheitsanalyse auf den durch den Auftraggeber zum Zweck der Durchführung schriftlich übermittelten IT-Systemen und/oder Applikationen des Auftraggebers erfolgt, bzw. erfolgen soll. Insoweit der Test nicht auf dem IT-System und/oder der Applikation des Auftraggebers erfolgt, versichert der Auftraggeber mit Unterzeichnung dieses Angebots, dass er das vollumfängliche und uneingeschränkte Recht zur Durchführung der technischen Sicherheitsanalyse auf den übermittelten IT-Systemen und/oder Applikationen hat. Auf Verlangen der usd AG hat der Auftraggeber nachzuweisen, dass er über das uneingeschränkte Recht zur Beauftragung der usd AG

zur Durchführung der technischen Sicherheitsanalyse und die Rechte für den Zugriff auf die übermittelten IT-Systeme und/oder Applikationen.

Vor der Durchführung der technischen Sicherheitsanalyse durch den Auftragnehmer, verpflichtet sich der Auftraggeber, sämtliche durch die usd AG zu prüfenden IT-Systeme und/oder Applikationen und die damit in Verbindung stehenden Daten vollumfänglich durch ein Backup zu sichern. Darüber hinaus hat der Auftraggeber sämtliche notwendigen Sicherheitsmaßnahmen, auch diejenigen, die über ein Backup hinausgehen, vor Nutzung der Dienstleistung zu treffen, um die IT-Systeme und/oder Applikationen und Daten notfalls nach der technischen Sicherheitsanalyse wieder in den ursprünglichen Zustand zurück versetzen zu können.

Der Auftraggeber stellt der usd AG abhängig von der Art der technischen Sicherheitsanalyse die zur – möglichst sicheren und schadlosen – Durchführung notwendigen Informationen und Unterlagen zur Verfügung. Vor Durchführung der technischen Sicherheitsanalyse wird die usd AG dem Auftraggeber mitteilen, welche Informationen benötigt werden. Der Auftraggeber wird der usd AG daraufhin die erforderlichen Informationen zeitgerecht, vollständig und richtig zu Verfügung stellen.

Der Auftraggeber benennt einen zuständigen Ansprechpartner, der sämtliche erforderlichen Fragen beantworten und alle damit zusammenhängenden Entscheidungen treffen kann.

Der Auftraggeber informiert mit angemessener Frist vor Durchführung der technischen Sicherheitsanalyse etwaig betroffene Dritte über die durchzuführende technische Sicherheitsanalyse, da bei einer technischen Sicherheitsanalyse auch IT-Systeme und/oder Applikationen Dritter, wie etwa der Router des Providers oder der Webserver eines Hosters, genutzt werden und nicht mit einer ausreichenden Sicherheit eine Beeinträchtigung des ordnungsgemäßen Betriebes dieser IT-Systeme und/oder Applikationen ausgeschlossen werden kann.

Der Auftraggeber wird ausdrücklich darauf hingewiesen, dass durch die technische Sicherheitsanalyse Schäden im bestehenden IT-System und/oder der Applikation auftreten können. Insbesondere können durch die technische Sicherheitsanalyse Beeinträchtigungen und Veränderungen auf der Webseite in Form von Layout-Veränderungen oder Beeinträchtigungen des Servers des Auftraggebers auftreten. Diese Schäden sind meist nur durch Backups, oder durch – teilweise umfangreiche – Nachbearbeitung durch den Auftraggeber zu beheben. Darüber hinaus wird der Auftraggeber darauf hingewiesen, dass das IT-System und/oder die Applikation des Auftraggebers während der technischen Sicherheitsanalyse möglicherweise nicht nutzbar ist.

Haftung, Haftungsbegrenzung, Haftungsausschluss

Die usd AG ist nicht verpflichtet zu überprüfen, ob der Auftraggeber die vollumfänglichen und uneingeschränkten Rechte an dem zu testenden IT-System und/oder der Applikation innehat.

Die usd AG haftet für Schäden, die der Auftraggeber erleidet, nur, soweit diese durch vorsätzliche oder grob

fahrlässige Handlungen oder durch die Verletzung wesentlicher Vertragspflichten verursacht worden sind. Im Falle der einfachen fahrlässigen Verletzung wesentlicher Vertragspflichten haftet die usd AG nur in Höhe des vorhersehbaren, vertragstypischen, unmittelbaren Durchschnittsschadens. Wesentliche Vertragspflichten sind solche, deren Erfüllung zur Erreichung des Ziels des Vertrags notwendig sind.

Die Haftung für Datenverluste wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrensprechender Anfertigung von Sicherungskopien eingetreten wäre. Die usd AG haftet nicht für solche Schäden, die darauf beruhen, dass der Kunde die technische Sicherheitsanalyse während der Ausführung unterbricht.

Die vorstehenden Regelungen gelten auch zu Gunsten der Mitarbeiter und sonstiger Erfüllungsgehilfen der usd AG.

Die vorstehenden Haftungsbeschränkungen und Ausschlüsse betreffen nicht die Ansprüche des Auftraggebers aufgrund einer Verletzung des Lebens, des Körpers, der Gesundheit und Ansprüche aufgrund der fahrlässigen Verletzung wesentlicher Vertragspflichten. Wesentliche Vertragspflichten sind solche, deren Erfüllung zur Erreichung des Ziels des Vertrags notwendig ist. Von dem Haftungsausschluss ebenfalls ausgenommen ist die Haftung aus Produkthaftung und für Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Anbieters, seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

Der usd AG steht der Einwand eines Mitverschuldens zu.

Die usd AG haftet nicht für einen mangelnden wirtschaftlichen Erfolg des Auftraggebers.

Macht höhere Gewalt (Naturkatastrophen, Krieg, Bürgerkrieg, Terroranschlag) die Leistungserbringung dauerhaft unmöglich, ist eine Leistungspflicht der usd AG ausgeschlossen, bereits an die usd AG gezahlte Honorare für noch nicht erbrachte Leistungen werden in diesem Fall zurückerstattet.

Freistellungsverpflichtung des Auftraggebers

Wird der Auftragnehmer von einem Dritten (z.B. ein Kunde des Auftraggebers) aufgrund etwaiger Auswirkungen der technischen Sicherheitsanalyse auf das IT-System und/oder die Applikation in Anspruch genommen, verpflichtet sich der Auftraggeber, den Auftragnehmer von jeglichen Ansprüchen freizustellen, sofern

(a) die technische Sicherheitsanalyse einem anerkannten und angemessenen Standard entsprach (andernfalls gilt „Haftung, Haftungsbegrenzung, Haftungsausschluss“ entsprechend) oder

(b) der Schaden aufgrund einer Pflichtverletzung des Auftraggebers (mit-)verursacht wurde, weil der Auftraggeber beispielsweise

- ein fremdes IT-System/eine fremde Applikation ohne entsprechende Erlaubnis hat testen lassen,
- betroffene Dritte nicht oder nicht mit angemessener Frist über die stattfindende technische Sicherheitsanalyse informiert wurden oder
- über keine datenschutzrechtliche Erlaubnis zur Übermittlung von personenbezogenen Daten verfügt hat.

Die Freistellungsverpflichtung bezieht sich auf alle Aufwendungen, die dem Auftragnehmer oder dessen einge-

setzten Mitarbeitern und sonstigen Erfüllungsgehilfen aus der außergerichtlichen, behördlichen und/oder gerichtlichen Inanspruchnahme durch einen Dritten notwendigerweise erwachsen. Der Auftraggeber hat dabei sämtliche Kosten und Gebühren für die notwendige rechtliche Verfolgung zu übernehmen, sowie sämtliche Schäden, Verluste und Ausgaben zu ersetzen.

Geheimhaltung

Die usd AG behandelt grundsätzlich überlassene Informationen vertraulich.

Datenschutz

Sofern die technische Sicherheitsanalyse eine Schwachstelle und/oder eine Sicherheitslücke des IT-Systems und/oder der Applikation aufdeckt, kann dies zur Folge haben, dass die Berater der usd AG Einsicht in die von dem Auftraggeber etwaig gespeicherten, personenbezogenen Daten nehmen. Die Einsichtnahme ist datenschutzrechtlich als Übermittlungsvorgang zu qualifizieren.

Mit Unterzeichnung dieses Angebots und durch Abgabe einer gesonderten Einwilligungserklärung, die Bestandteil des intendierten Vertrages ist, versichert der Auftraggeber, dass er zur etwaigen Übermittlung von personenbezogenen Daten berechtigt ist. Andernfalls schließt der Auftraggeber die Einsichtnahme von personenbezogenen Daten durch geeignete Maßnahmen (z.B. Pseudonymisierung, Anonymisierung) aus.

Die usd hat alle Mitarbeiter, die mit der Vertragserfüllung betraut sind, auf die strenge Einhaltung der anwendbaren datenschutzrechtlichen Vorschriften verpflichtet. Etwaige durch die technische Sicherheitsanalyse eingesehene personenbezogene Daten

wird die usd AG nicht speichern oder nur speichern, nutzen oder verarbeiten, soweit und solange dies zur Erfüllung dieses Vertrages zwingend erforderlich ist.

Im Übrigen erfolgt jede weitere Verarbeitung von personenbezogenen Daten durch die usd ausschließlich auf Weisung des Auftraggebers. Der Auftragnehmer darf die Daten des Auftraggebers nur im Rahmen dieser Weisung verarbeiten oder nutzen. Auf Anforderung des Auftraggebers oder im Zweifelsfall werden die Parteien einen gesonderten Auftragsdatenverarbeitungsvertrag abschließen.

Widerspruch AGB/Einkaufsbedingungen

Gegenbestätigungen des Auftraggebers unter Hinweis auf ihre eigenen Geschäfts- und/oder Einkaufsbedingungen wird hiermit widersprochen. Individuelle Vereinbarungen bleiben hiervon unberührt.

Schlussbestimmungen

Alle Anhänge dieses Angebots sind Bestandteil des intendierten Vertrages. Dieses Angebot stellt nach Unterzeichnung mit seinen inkludierten Anhängen die vollständige und ganze Vereinbarung der Parteien zu diesem Vertragsgegenstand (technische Sicherheitsanalyse) dar. Nachfolgende individuelle Vereinbarungen bleiben hiervon unberührt.

Es gilt ausschließlich das Recht der Bundesrepublik Deutschland unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG).

Der ausschließliche Gerichtsstand ist Frankfurt am Main in der Bundesrepublik Deutschland, soweit der Auftraggeber Kaufmann ist. Der Auftragnehmer ist daneben berechtigt, auch im allgemeinen Gerichtsstand des Nutzers zu klagen.

Die Unwirksamkeit einer oder mehrerer Bestimmungen dieses Vertrages berührt nicht die Wirksamkeit dieses Vertrages im Übrigen.