



## **Sicherheit im Überblick**

Letzte Aktualisierung: Oktober 2019



# Inhaltsverzeichnis

1	Unser Unternehmen und unsere Produkte	3
2	Sicherheit und Risikobeherrschung bei HubSpot	3
3	Unsere Ziele für das Sicherheits- und Risikomanagement	3
4	Sicherheitsmechanismen von HubSpot	4
4.1	Produktinfrastruktur von HubSpot	4
4.1.1	Sicherheit in Rechenzentren	4
4.1.2	Netzwerksicherheit und Perimeterschutz	4
4.1.3	Konfigurationsmanagement	5
4.1.4	Alarmierung und Überwachung	5
4.1.5	Zugriff auf die Infrastruktur	6
4.2	Schutz von Anwendungen	6
4.2.1	Bedrohungsabwehr bei Web-Anwendungen	6
4.2.2	Entwicklungs- und Release-Verwaltung	7
4.2.3	Schwachstellen-Scans, Penetrationstests und Bug-Bounty-Prämien	7
4.3	Schutz von Kundendaten	8
4.3.1	Vertrauliche Informationen in den HubSpot-Produkten	8
4.3.2	Schutz von Kreditkarteninformationen	8
4.3.3	Verschlüsselung bei der Übermittlung und im Speicher	9
4.3.4	Schutzmaßnahmen bei der Benutzeranmeldung	9
4.3.5	Benutzer- und API-Autorisierung	9
4.3.6	Zugriff durch HubSpot-Mitarbeiter	10
4.4	Datenschutz	10
4.4.1	Datenaufbewahrungsrichtlinie	11
4.4.2	Verwaltung des Datenschutzprogramms	11
4.5	Geschäftskontinuität und Disaster Recovery	11
4.5.1	Zuverlässigkeit und Wiederherstellung von Systemen	11
4.5.2	Datensicherungsstrategie	12
4.6	Unternehmenssicherheit bei HubSpot	12
4.6.1	Mitarbeiterauthentifizierung und -autorisierung	12
4.6.2	Zugriffsverwaltung	13
4.6.3	Hintergrundüberprüfungen	13



4.6.4	Physische Unternehmenssicherheit bei HubSpot	13
4.6.5	Anbietermanagement	14
4.6.6	Sicherheitsbewusstsein und Sicherheitsrichtlinien	14
4.7	Vorfallmanagement	14
5	Produktsicherheitsfunktionen	15
5.1	Marketing Hub	15
5.2	HubSpot CRM	16
5.3	Sales Hub	16
5.4	Service Hub	17
6	Compliance	17
7	Umfang und Verwendung dieses Dokuments	18



# Sicherheit bei HubSpot – Übersicht

## 1 UNSER UNTERNEHMEN UND UNSERE PRODUKTE

HubSpot ist die weltweit führende Plattform für Inbound-Marketing, Vertrieb und Kundenservice. Seit 2006 stellt HubSpot umfassende Lösungen für Marketing, Vertrieb und Kundenservice bereit. Heute vertrauen Zehntausende Unternehmen in mehr als 90 Ländern auf die Software, Services und Supportdienste von HubSpot, um in Sachen Kundengewinnung, -interaktion und -bindung neue Maßstäbe zu setzen. Die Inbound-Marketing-Software von HubSpot belegte bei VentureBeat, GetApp, Capterra und G2Crowd den ersten Platz und vereint Social-Media-Publishing und -Überwachung, Funktionen zum Bloggen, SEO, Verwaltung von Website-Content, E-Mail-Marketing sowie Berichterstattungs- und Analytics-Funktionen in einer integrierten Plattform. Sales Hub und HubSpot CRM, die preisgekrönten Vertriebsanwendungen von HubSpot, ermöglichen Vertriebs- und Serviceteams, gezielt mit Leads sowie potenziellen und bestehenden Kunden zu kommunizieren. Service Hub ist die optimale Lösung, um reibungslose und durchwegs positive Kundenerfahrungen zu schaffen.

Die HubSpot-Produkte sind als Software-as-a-Service-Lösungen (SaaS) erhältlich. Kunden können über eigens zu diesem Zweck entwickelte Webanwendungen, Programmierschnittstellen (APIs) und E-Mail-Plug-ins auf diese Lösungen zugreifen.

## 2 SICHERHEIT UND RISIKOBEHERRSCHUNG BEI HUBSPOT

Im Mittelpunkt der Sicherheitsstrategie von HubSpot steht der Schutz von Kunden- und Benutzerdaten. Aus diesem Grund hat HubSpot in geeignete Ressourcen und Kontrollverfahren investiert, die gewährleisten, dass wir unseren Kunden einen hochwertigen und vor allem sicheren Service bieten können. In diesem Zusammenhang wurden auch ein spezielles Enterprise- sowie ein Produkt-Sicherheitsteam etabliert. Diese Teams sind für das umfassende Sicherheitsprogramm von HubSpot sowie den Governance-Prozess zuständig. Zu unseren Hauptaufgaben zählen die Erstellung neuer und die Optimierung bestehender Kontrollmechanismen, die Implementierung und Verwaltung des Sicherheitsprogramms von HubSpot sowie die Entwicklung einer unterstützenden Struktur für die Durchführung eines effizienten Risikomanagements. Unser Chief Security Officer, der dem Chief Operating Officer untersteht, ist für die Implementierung von Sicherheits- und Schutzmaßnahmen bei HubSpot und allen dazugehörigen Produkten zuständig.

## 3 UNSERE ZIELE FÜR DAS SICHERHEITS- UND RISIKOMANAGEMENT

Unser Sicherheitsprogramm wurde auf der Grundlage der Best Practices der SaaS-Branche entwickelt. Zu unseren wichtigsten Zielen gehören:

- Kundenvertrauen und -schutz: Wir sind bestrebt, unseren Kunden unter Berücksichtigung von Datenschutz und der Vertraulichkeit ihrer Informationen stets erstklassige Produkte und einen herausragenden Service zu bieten.
- Verfügbarkeit und Kontinuität von Diensten: Wir gewährleisten autorisierten Kunden eine ständige Verfügbarkeit von Diensten und Daten und arbeiten proaktiv an der Minimierung jeglicher Sicherheitsrisiken, die Serviceunterbrechungen bedingen könnten.
- Informations- und Serviceintegrität: Wir stellen sicher, dass die Daten unserer Kunden weder korumpiert noch in unangemessener Weise verändert werden.
- Einhaltung von Standards: Wir implementieren Verfahren und Kontrollmechanismen, um geltende internationale rechtliche Bestimmungen und branchenübliche Best-Practice-Ansätze zu



erfüllen. Wir haben unser Sicherheitsprogramm auf der Grundlage der branchenüblichen Richtlinien für Cloud-Sicherheit erstellt. Wir wenden beispielsweise Standards an wie COBIT und Cloud Security Alliance CCM und orientieren unsere Praktiken an den Normen ISO 27001 und NIST SP 800-53.

## 4 SICHERHEITSMECHANISMEN VON HUBSPOT

Um die uns anvertrauten Daten zu schützen, haben wir eine Reihe von Sicherheitsmechanismen eingerichtet. Die Sicherheitsmechanismen von HubSpot sind so konzipiert, dass sie eine hohe Mitarbeitereffizienz ohne künstliche Hemmnisse ermöglichen und gleichzeitig das Risiko minimieren. In den folgenden Abschnitten werden einige dieser Kontrollmechanismen beschrieben. Sämtliche Einzelheiten zum Sicherheitsprogramm von HubSpot finden Sie auf <https://www.hubspot.de/security>.

### 4.1 PRODUKTINFRASTRUKTUR VON HUBSPOT

#### 4.1.1 SICHERHEIT IN RECHENZENTREN

Die Produktinfrastruktur von HubSpot wird bei führenden Anbieter für Cloud-Infrastrukturen gehostet. Dabei werden vorwiegend Amazon Web Services (AWS) und Google Cloud Platform (GCP) genutzt. Diese Lösungen bieten ein hohes Maß an physischer Sicherheit und Netzwerksicherheit und HubSpot ist so nicht von einem bestimmten Hosting-Anbieter abhängig. Derzeit befinden sich die AWS-Cloud-Serverinstanzen an verschiedenen Standorten in den USA. Die GCP-Cloud-Instanzen werden in Deutschland gehostet. Beide Anbieter befolgen ein geprüftes Sicherheitsprogramm, das Compliance mit SOC 2 und ISO 27001 umfasst. HubSpot hostet keine Produktsysteme an seinen eigenen Unternehmensstandorten.

Diese erstklassigen Infrastrukturanbieter nutzen die modernste verfügbare Gebäudeinfrastruktur im Hinblick auf Stromversorgung, Netzwerktechnologie und Sicherheit. Unsere Anbieter gewährleisten Betriebszeiten ihrer Anlagen von 99,95 % bis 100 %. Zudem wird für diese Anlagen eine Mindestredundanz von N+1 für sämtliche Stromversorgungs-, Netzwerk- und Heizungs-/Klimaanlagendienste garantiert. Sowohl der physische als auch der elektronische Zugang zu den Standorten dieser Anbieter – über öffentliche (Internet) oder private (Intranet) Netzwerke – ist strikt beschränkt, um jegliche unerwünschte Unterbrechungen der Dienste für unsere Kunden zu vermeiden.

Die physischen, umgebungsbedingten und infrastrukturellen Sicherheitsmaßnahmen, einschließlich Kontinuitäts- und Wiederherstellungsplänen, wurden im Rahmen der SOC 2 Typ II und ISO 27001 Zertifizierungen unabhängig validiert. Zertifikate sind auf der [AWS-Compliance-Seite](#) und der [Sicherheitswebseite der Google Cloud Platform](#) zu finden.

#### 4.1.2 NETZWERKSICHERHEIT UND PERIMETERSCHUTZ

Die Produktinfrastruktur von HubSpot wurde im Hinblick auf internetfähige Schutzmaßnahmen entwickelt. Insbesondere wurde der Netzwerkschutz so konzipiert, dass unbefugte Netzwerkzugriffe auf die Produktinfrastruktur und innerhalb der internen Produktinfrastruktur verhindert werden. Diese Kontrollmechanismen umfassen Listen für die Routing- und Netzwerkzugriffssteuerung (Firewallschutz) der Enterprise-Klasse.

In AWS Virtual Private Cloud (VPC)-Sicherheitsgruppen oder GCP-Firewall-Regeln wurden Zugriffssteuerungslisten auf Netzwerkebene implementiert. Dadurch werden alle Serverinstanzen in der Infrastruktur auf Port- und Adressebene geschützt. Diese Firewall-Technologien verweigern standardmäßig unbeabsichtigten Traffic, und der gesamte Netzwerk-Traffic wird protokolliert und vom Überwachungssystem geprüft (mehr dazu in [Abschnitt 4.1.4](#)). Diese Netzwerk-Zugriffsregeln ermöglichen eine detaillierte Kontrolle des Netzwerk-Traffics im öffentlichen Netzwerk sowie zwischen



Serverinstanzen innerhalb der Infrastruktur. Innerhalb der Infrastruktur ermöglichen interne Netzwerkbeschränkungen eine mehrschichtige Vorgehensweise, um sicherzustellen, dass nur genehmigte Geräte miteinander kommunizieren können.

Änderungen des Netzwerksicherheitsmodells werden aktiv überwacht und durch standardmäßige Änderungskontrollprozesse gesteuert. Alle bestehenden Regeln und Änderungen werden auf Sicherheitsrisiken geprüft und entsprechend erfasst.

#### *4.1.3 KONFIGURATIONSMANAGEMENT*

Durch Automatisierung sind wir in der Lage, unsere Vorkehrungen entsprechend den Anforderungen unserer Kunden zu skalieren. Die Produktinfrastruktur ist eine hochautomatisierte Umgebung, in der die Kapazitäten und Fähigkeiten nach Bedarf flexibel erweitert werden können. Serverinstanzen verwenden eine Puppet-Infrastruktur, d. h. sämtliche Serverkonfigurationen werden von der Inbetriebnahme bis zur Ausrangierung streng kontrolliert.

Alle Servertyp-Konfigurationen werden in Images und Puppet-Konfigurationsdateien eingebettet. Das Konfigurationsmanagement auf der Serverebene erfolgt beim Serveraufbau mithilfe dieser Images und Konfigurationsskripts. Änderungen an der Konfiguration und den Standard-Images werden durch einen kontrollierten Änderungssteuerungsprozess gesteuert. Jeder Instanztyp enthält je nach Bereitstellung der Instanz eine eigene festgeschriebene Konfiguration.

Die Patch-Verwaltung und Konfigurationssteuerung erfolgt in der Regel durch das Entfernen von Serverinstanzen, die nicht mehr mit dem erwarteten Grundschutz konform sind und der Bereitstellung einer Ersatzinstanz an ihrer Stelle. Unsere täglichen Infrastrukturprozesse beinhalten eine rigorose und automatisierte Konfigurationsverwaltung.

#### *4.1.4 ALARMIERUNG UND ÜBERWACHUNG*

Bei HubSpot sind die Server-Erstellungsverfahren komplett automatisiert. Zusätzlich investieren wir intensiv in Technologien für automatische Überwachung, Alarmierung und Reaktion, um potenzielle Probleme kontinuierlich zu beheben. Die Produktinfrastruktur von HubSpot ist so konzipiert, dass Techniker und Administratoren gewarnt werden, wenn Anomalien auftreten. So lösen zum Beispiel Fehlerraten, Missbrauchsszenarien, Angriffe auf Anwendungen und andere Anomalien automatische Reaktionen und Warnungen an die zuständigen Teams aus, damit diese reagieren und das Problem untersuchen und beheben können. Beim Auftreten von unerwarteten oder böswilligen Aktivitäten werden die entsprechenden Fachkräfte benachrichtigt, um zu gewährleisten, dass Probleme rasch behoben werden können.

Zudem sind viele automatisierte Trigger in das System eingebaut, um auf vorhersagbare Situationen sofort reagieren zu können. Die Blockierung des Datenverkehrs, Quarantäne, Prozessbeendigung und ähnliche Funktionen werden bei vordefinierten Schwellenwerten auf den Plan gerufen und gewährleisten, dass sich die HubSpot-Plattform selbst gegen ein breites Spektrum unerwünschter Situationen schützen kann.

Die Fähigkeit zur Erkennung von und Reaktion auf Anomalien verdankt HubSpot einem Rund-um-die-Uhr-Überwachungsprogramm und detaillierter Protokollierung. Unsere Systeme erfassen und speichern Protokolle, die sämtliche Technologien unserer Produkte einschließen. Auf Anwendungsebene werden ebenfalls alle Anmeldungen, Seitenaufrufe, Änderungen und sonstigen Zugriffe auf HubSpot-Portale protokolliert. Im Back-End der Infrastruktur protokollieren wir Authentifizierungsversuche, horizontale und vertikale Berechtigungsänderungen, den Zustand der Infrastruktur, verarbeitete Anfragen sowie



viele weitere Befehle und Transaktionen. Protokolle und Ereignisse werden in Echtzeit überwacht, und Ereignisse werden unverzüglich und zu jeder Tageszeit an Entwickler, Sicherheitsfachleute und Techniker weitergeleitet, damit diese geeignete Maßnahmen ergreifen können.

#### **4.1.5 ZUGRIFF AUF DIE INFRASTRUKTUR**

Ganze Kategorien potenzieller Sicherheitsereignisse werden dank eines strengen, einheitlichen und ausgeklügelten Modells zur Zugriffssteuerung verhindert. Das bedeutet, dass der Zugriff auf die Systeme von HubSpot einer strengen Kontrolle unterliegt. HubSpot-Mitarbeiter erhalten Zugang zu unternehmensinternen Services, Vertriebs- und Marketingportalen von HubSpot sowie der Produktinfrastruktur. Der Zugriff wird dabei unter Berücksichtigung der Funktion eines Mitarbeiters auf der Grundlage eines rollenbasierten Zugriffssteuerungsmodells gewährt. Weitere Informationen zum rollenbasierten Zugriffssteuerungsmodell von HubSpot innerhalb des Unternehmens finden Sie in Abschnitt 4.3.

Der Zugriff auf Infrastrukturtools, Server und ähnliche Services ist auf die Mitarbeiter beschränkt, deren Funktion einen Zugriff erfordert. Für den Notfallzugriff und den Zugriff auf Verwaltungsfunktionen verwendet das HubSpot-System ein Just-In-Time-Access (JITA)-Modell, bei dem Benutzer den Zugriff auf berechtigungsbasierte Funktionen für eine begrenzte Dauer beantragen können.

Benutzern werden die entsprechenden Berechtigungen zugewiesen, um JITA-Anträge nach Geschäftsbereich und Team stellen zu können. Ist ein außergewöhnlicher Notfallzugriff erforderlich, wie beispielsweise ein Sudo-Zugriff auf einen Linux-Server, stellt der Benutzer einen entsprechenden JITA-Antrag. Der JITA-Antrag wird protokolliert. Protokolle werden kontinuierlich auf anomale Anfragen hin überwacht. Der Zugriff auf die berechtigungsbasierte Funktion wird gewährt, sodass die Person ihre Arbeit erledigen kann.

Darüber hinaus sind direkte Netzwerkverbindungen zu Produktinfrastruktur-Geräten über SSH oder ähnliche Protokolle verboten. Entwickler und Techniker müssen sich zuerst über einen Bastion-Host oder einen „Jump-Server“ authentifizieren, bevor sie auf Qualitätssicherungs- oder Produktionsumgebungen zugreifen können. Die Authentifizierung auf Serverebene nutzt benutzerspezifische eindeutige SSH-Schlüssel und eine tokenbasierte Zwei-Faktor-Authentifizierung.

## **4.2 SCHUTZ VON ANWENDUNGEN**

### **4.2.1 BEDROHUNGSABWEHR BEI WEB-ANWENDUNGEN**

Bei HubSpot haben wir uns dazu verpflichtet, die Daten und Websites unserer Kunden zu schützen. Daher nutzen wir eine in der Branche anerkannte Web Application Firewall (WAF). Die WAF erkennt Angriffe auf die Produkte von HubSpot oder auf die Websites von HubSpot-Kunden, die auf der Plattform gehostet werden, automatisch und wehrt diese ab. Die WAF von HubSpot schützt den Zugriff auf die HubSpot-Plattform (z. B. die Funktionen, auf die Sie unter <https://app.hubspot.com> oder durch eine Integration mit APIs unter <https://api.hubapi.com> zugreifen können). Zusätzlich werden auch alle Kundinhalte, die auf der Plattform gehostet werden, automatisch geschützt. Die für die Erkennung und Blockierung von böswilligem Traffic angewandten Regeln sind auf die Richtlinien und Best Practices abgestimmt, die vom Open Web Application Security Project (OWASP) in den OWASP Top 10 und



vergleichbaren Empfehlungen dokumentiert sind. Auch Schutzmaßnahmen gegen Distributed Denial of Service (DDoS)-Angriffe wurden eingerichtet. Diese tragen dazu bei, dass die Websites der Kunden und andere Teile der HubSpot-Produkte durchgehend verfügbar sind.

Die WAF ist auf Basis einer Kombination aus branchenüblichen und benutzerdefinierten Regeln konfiguriert, die automatisch die richtigen Sicherheitsfunktionen für einen optimalen Schutz unserer Kunden aktivieren oder deaktivieren kann. Diese Tools überwachen aktiv den Echtzeit-Datenverkehr auf der Anwendungsebene und können ausgehend von Art und Frequenz des beobachteten Verhaltens Warnmeldungen zu schadhaftem Verhalten ausgeben oder Dienste verweigern.

#### **4.2.2 ENTWICKLUNGS- UND RELEASE-VERWALTUNG**

Die schnelle Weiterentwicklung der Funktionen unserer Software ist eines der Charakteristika, die HubSpot auszeichnen. Dank eines modernen Softwareentwicklungsansatzes mit kontinuierlicher Bereitstellung können wir unseren Kunden Produkte anbieten, die laufend verbessert und ausgebaut werden. Jeden Tag werden Tausende Erweiterungen des Programmcodes vorgeschlagen, genehmigt, zusammengeführt und bereitgestellt. Der Code wird bereits während der Entwicklung von spezialisierten Teams, die die HubSpot-Plattform bis ins Detail kennen, überprüft und einer Qualitätssicherung unterzogen. Genehmigungen werden von den Verantwortlichen für die jeweiligen Repositories kontrolliert. Nachdem der Code genehmigt wurde, wird er automatisch an die kontinuierliche Integrationsumgebung von HubSpot übermittelt. Dort erfolgen Kompilierung, Bündelung und Tests. Wenn der neue Code alle Kontrollen bestanden hat, wird er automatisch in der Anwendungsebene bereitgestellt.

Bei der Bereitstellung von neuem Code werden Archive mit dem bisherigen in der Live-Umgebung verwendeten Code erstellt, für den Fall, dass Fehler bei den nach der Veröffentlichung ausgeführten Hooks erkannt werden. Das für die Bereitstellung verantwortliche Team verwaltet Mitteilungen zum Zustand seiner Anwendungen. Wenn ein Fehler auftritt, wird sofort ein Roll-Back ausgelöst.

Im Rahmen dieses kontinuierlichen Modells können wir Funktionen mithilfe umfassenden Software-Gatings und Traffic-Managements auf Basis von Kundenpräferenzen steuern (private Beta-Version, öffentliche Beta-Version, Veröffentlichung der Live-Version). Wesentliche Änderungen an den Funktionen werden entweder über In-App-Benachrichtigungen und/oder [Beiträge zu Produkt-Updates](#) kommuniziert.

Neu entwickelter Code wird zuerst in der eigens dazu eingerichteten, separaten Qualitätssicherungsumgebung von HubSpot bereitgestellt, wo er letzten Tests unterzogen wird, bevor er schließlich in die Produktionsumgebung gelangt. Die Segmentierung auf Netzwerkebene verhindert dabei unbefugten und unerwünschten Zugriff von der Qualitätssicherungs- oder Produktionsumgebung aus. In der Qualitätssicherungsumgebung werden keine Kundendaten verwendet. Auch bei anderen Tests kommen keinerlei Kundendaten zum Einsatz.

#### **4.2.3 SCHWACHSTELLEN-SCANS, PENETRATIONSTESTS UND BUG-BOUNTY-PRÄMIEN**

Das Sicherheitsteam von HubSpot arbeitet bei den Schwachstellen-Scans mit einem Ansatz mit mehreren Ebenen. Dabei werden diverse branchenübliche Werkzeuge angewendet, um eine umfassende Abdeckung unseres Technologiebestands zu gewährleisten. Wir führen laufend eine Vielzahl verschiedener Schwachstellen-Scans und Penetrationstests unserer Technologien durch. Diese



umfassen kontinuierliche Schwachstellen-Scans für unsere internen Netzwerke, Anwendungen und unsere Unternehmensinfrastruktur. Netzwerkbasierte Schwachstellen-Scans auf der Anwendungsebene werden mindestens täglich ausgeführt, um zu gewährleisten, dass wir die neuesten Schwachstellen erkennen und entsprechende Maßnahmen ergreifen. Mittels statischer Code-Analysen wird automatisch der aktuellste Code überprüft, um potenzielle Sicherheitslücken bereits frühzeitig im Entwicklungszyklus zu erkennen.

Ständig laufende Scans, adaptive Scan-Aufnahmelisten und laufende Aktualisierung der Schwachstellen-Signaturen helfen HubSpot als präventive Maßnahmen gegen viele Sicherheitsbedrohungen. Zur externen Überprüfung unserer Fähigkeit zur Erkennung und Abwehr von Sicherheitsrisiken lassen wir viermal jährlich Penetrationstests von branchenweit anerkannten externen Anbietern durchführen. Ziel dieser Programme ist es, Schwachstellen, die ein Sicherheitsrisiko darstellen, mithilfe iterativer Prüfungen zu erkennen und mögliche Probleme schnellstmöglich zu beheben. Mit Penetrationstests werden die Anwendungsebenen und Netzwerkebenen des Technologiebestands von HubSpot getestet. Dabei erhalten die Prüfer internen Zugriff auf die Produkt- und/oder Unternehmensnetzwerke von HubSpot, um eine möglichst umfassende Bandbreite möglicher Angriffsszenarien testen zu können.

Zusätzlich zu Schwachstellen-Scans und unabhängigen Penetrationstests betreibt HubSpot auch ein eigenes Bug-Bounty-Programm. Unabhängige Sicherheitsexperten werden gebeten, HubSpot-Produkte auf Sicherheitslücken hin zu untersuchen und diese zu melden. Meldungen werden von HubSpot entsprechend vergütet. Sicherheitstests von Testportalen durch Mitglieder der Security-Community und HubSpot-Kunden werden ausdrücklich begrüßt. Informationen über das Bug-Bounty-Programm von HubSpot sind unter <https://bugcrowd.com/hubspot> verfügbar.

## 4.3 SCHUTZ VON KUNDENDATEN

### 4.3.1 VERTRAULICHE INFORMATIONEN IN DEN HUBSPOT-PRODUKTEN

Die HubSpot-Produkte bieten ein integriertes Marketing-, Vertriebs- und Kundenservice-Erlebnis. Bei den von uns erfassten Daten handelt es sich um Daten, die aus Interaktionen mit Leads oder Kunden, öffentlichen Verzeichnissen und anderweitigen vertrauenswürdigen Quellen stammen. Die HubSpot-Tools ermöglichen es Kunden, selbst festzulegen, welche Daten erfasst und für sie gespeichert werden sollen. Gemäß den [Nutzungsbedingungen](#) und der [Richtlinie zur akzeptablen Nutzung](#) von HubSpot tragen unsere Kunden Sorge dafür, dass sie ausschließlich Daten erfassen, die zur Förderung ihrer Marketing-, Vertriebs- und Kundenservice-Prozesse angemessen sind. Die HubSpot-Produkte werden nicht zur Erfassung sensibler Daten wie Kredit- oder Bankkartennummern, Informationen zu privaten Bankkonten, Sozialversicherungsnummern, Reisepassnummern, Führerscheinnummern oder ähnlichen Identifikationsdaten sowie Finanzauskünfte oder Daten zur Beschäftigung oder Gesundheit eingesetzt.

### 4.3.2 SCHUTZ VON KREDITKARTENINFORMATIONEN

Viele HubSpot-Kunden zahlen den Service per Kreditkarte. Die von Kunden übermittelten Kreditkartendaten werden von HubSpot nicht gespeichert, bearbeitet oder erfasst. Wir arbeiten mit vertrauenswürdigen und PCI-zertifizierten Zahlungsanbietern zusammen, um eine sichere Verarbeitung der Kreditkartendaten unserer Kunden zu gewährleisten, die den geltenden Vorschriften und Branchenstandards entspricht.



### 4.3.3 VERSCHLÜSSELUNG BEI DER ÜBERMITTLUNG UND IM SPEICHER

Sämtliche sensiblen Interaktionen mit den HubSpot-Produkten (z. B. API-Aufrufe, Anmeldung, authentifizierte Sitzungen beim Portal eines Kunden usw.) werden bei der Übermittlung mit TLS 1.0, 1.1, 1.2 oder 1.3 und mindestens 2.048-Bit-Schlüsseln verschlüsselt. Transport Layer Security (TLS) ist für Kunden, die ihre Websites auf der HubSpot-Plattform hosten, standardmäßig verfügbar. In unserem [Leitfaden für die Einrichtung von Websites](#) finden Sie weitere Informationen zum Konfigurieren von TLS. Kunden, die die Verschlüsselungsprotokolle für HTTPS-Verbindungen beschränken möchten, können sich diesbezüglich mit dem Kundensupport oder ihrem Customer Success Manager in Verbindungen setzen.

Bei HubSpot werden verschiedene Technologien eingesetzt, um die Verschlüsselung von Daten im Speicher zu gewährleisten. Für physische und virtualisierte Festplatten, die von HubSpot-Produktserverinstanzen genutzt werden, sowie langfristige Speicherlösungen wie AWS S3 wird AES-256-Verschlüsselung verwendet. Zusätzlich werden bestimmte Datenbanken oder Informationen auf Feldebene im Speicher abhängig vom Sensibilitätsgrad der Daten verschlüsselt. Zum Beispiel werden Benutzerpasswörter gehasht, und bestimmte E-Mail-Funktionen verschlüsseln Nachrichtendaten sowohl im Speicher als auch bei der Übermittlung.

Verschlüsselungsschlüssel für die Verschlüsselung sowohl im Speicher als auch bei der Übermittlung werden von der HubSpot-Plattform sicher verwaltet. Private TLS-Schlüssel für die Verschlüsselung bei der Übermittlung werden über unseren Content-Delivery-Partner verwaltet. Verschlüsselungsschlüssel auf Volume- oder Feldebene für die Verschlüsselung im Speicher werden in einem gehärteten Key Management System (KMS) aufbewahrt. Die Schlüssel rotieren regelmäßig, wobei die Schlüsselart sowie der Sensibilitätsgrad des Schlüssels und der damit geschützten Daten für die Häufigkeit der Rotation ausschlaggebend sind. Grundsätzlich laufen TLS-Zertifikate nach zwei Jahren ab.

### 4.3.4 SCHUTZMAßNAHMEN BEI DER BENUTZERANMELDUNG

Die HubSpot-Produkte ermöglichen es Benutzern, sich über die integrierte HubSpot-Anmeldung, über die Option „Mit Google anmelden“ oder mittels Single-Sign-On bei ihren HubSpot-Konten anzumelden. Die integrierte Anmeldeoption schreibt eine einheitliche Kennwortrichtlinie vor, laut der ein Kennwort aus mindestens acht Zeichen bestehen muss. Dabei muss es sich um eine Kombination aus Groß- und Kleinbuchstaben, Sonderzeichen, Leerzeichen und Zahlen handeln. Benutzer, die die integrierte HubSpot-Anmeldung nutzen, können die Standard-Kennwortrichtlinie nicht ändern. Kunden, die einen SSO-Anbieter (Single-Sign-On) nutzen, können eine SSO-basierte Anmeldung für ihre Benutzer einrichten. Anleitungen zum [Einrichten von SSO finden Sie in der HubSpot Academy](#). Benutzer, die sich mittels Single-Sign-On oder über Google anmelden, können bei ihrem SSO-Anbieter oder in ihren Google-Konten eigene Kennwortrichtlinien konfigurieren.

Kunden, die die integrierte HubSpot-Anmeldung nutzen, wird empfohlen, eine [zweistufige Authentifizierung](#) für ihre HubSpot-Konten einzurichten. Darüber hinaus können Portaladministratoren über die Konfiguration ihrer HubSpot-Portale sicherstellen, dass die zweistufige Authentifizierung bei allen Benutzern aktiviert ist.

### 4.3.5 BENUTZER- UND API-AUTORISIERUNG



Kunden können für ihre Konten genau definierte Zugriffsberechtigungen zuweisen und den Zugriff auf Datenfunktionen beschränken. Weitere Informationen zu Benutzerrollen finden Sie im [Leitfaden für Benutzerrollen und -berechtigungen in HubSpot](#).

Der Zugriff auf die Programmierschnittstelle (API) ist entweder über API-Schlüssel- oder OAuth (Version 2)-Autorisierung möglich. Kunden können dazu API-Schlüssel für ihre Portale generieren. Die Schlüssel ermöglichen eine rasche Prototypenerstellung für benutzerspezifische Integrationen. Die OAuth-Implementierung von HubSpot bietet eine striktere Authentifizierung und Autorisierung von API-Anfragen. Darüber hinaus ist OAuth für alle Integrationen erforderlich, die von HubSpot auf seiner Website vorgestellt werden. Die Autorisierung von OAuth-fähigen Anforderungen erfolgt im Rahmen festgelegter Umfänge. Weitere Informationen zur API-Nutzung finden Sie im [Entwickler-Portal auf HubSpot.com](#) (auf Englisch).

#### 4.3.6 ZUGRIFF DURCH HUBSPOT-MITARBEITER

HubSpot regelt den Datenzugriff einzelner Benutzer in der Produktions- und Unternehmensumgebung. Einige befugte HubSpot-Mitarbeiter erhalten je nach ihrer Rolle Zugriff auf Daten aus Produktionsumgebungen, entweder durch rollenbasierte Zugriffssteuerung (RBAC) oder bei Bedarf via JITA („Just in Time Access“).

Technikern und Mitgliedern von Operations-Teams kann entsprechend ihrer Rolle Zugriff auf verschiedene Systeme aus Produktionsumgebungen gewährt werden. In den meisten Fällen dient der Zugriff der Bearbeitung von Warnmeldungen und Fehlerbehebungen sowie der Analyse von Informationen für Entscheidungen zu Produktinvestitionen oder Produktsupport. Der Zugriff auf die Produktinfrastruktur wird mit Netzwerkzugriffssteuerungen sowie Benutzerauthentifizierungs- und -autorisierungssteuerungen eingeschränkt. Der Zugriff auf Netzwerkfunktionen ist strikt auf Personen beschränkt, deren Funktion einen Zugriff erforderlich macht, und wird kontinuierlich überprüft.

Mitarbeiter, die im Kundensupport, in Service-Teams oder in sonstiger Weise in der Kundenbetreuung tätig sind und berechtigungsbasierten Zugriff benötigen, können innerhalb eines befristeten Zeitraums eine Just-in-Time-Authentifizierung (JITA) für den Zugriff auf Endkunden-Portale anfordern. Anträge für den Zugriff sind auf die Aufgaben der Mitarbeiter im Rahmen ihrer Support- und Kundenserviceverpflichtungen beschränkt. Die Anträge sind auf den punktuellen, befristeten Zugang zum Portal eines spezifischen Kunden für maximal 24 Stunden beschränkt. Alle Zugriffsanträge, Anmeldungen, Anfragen, Seitenaufrufe und ähnliche Informationen werden protokolliert.

Alle Zugriffsanträge, Anmeldungen, Anfragen, Seitenaufrufe und ähnlichen Informationen werden protokolliert. Es erfolgt eine tägliche automatisierte Überprüfung und eine mindestens halbjährliche Neuzertifizierung, um sicherzustellen, dass die gewährte Autorisierung den Rollen und jeweiligen Tätigkeiten der Mitarbeiter angemessen sind.

## 4.4 DATENSCHUTZ

Der Schutz der Daten unserer Kunden hat für HubSpot höchste Priorität. Wie in unserer [Datenschutzrichtlinie](#) dargelegt, verkaufen wir Ihre personenbezogenen Daten niemals an Dritte. Der in diesem Dokument beschriebene Schutz und weitere von uns implementierte Schutzmaßnahmen wurden mit dem Ziel konzipiert, dass Ihre Daten geheim bleiben und vor Manipulationen geschützt sind.



Bei der Entwicklung und Erstellung der Produkte von HubSpot stehen die Bedürfnisse und der Schutz der Daten unserer Kunden im Vordergrund. Unser Datenschutzprogramm umfasst Best Practices, die Anforderungen unserer Kunden und deren Kontakte sowie regulatorische Vorschriften.

HubSpot ist zudem gemäß dem EU-US- und dem Swiss-US-Privacy-Shield-Framework zertifiziert. Weitere Informationen zu unserer Zertifizierung sind auf der [Website zum Privacy Shield](#) verfügbar. HubSpot hat außerdem eine [TRUSTe-Zertifizierung für Unternehmensdatenschutz](#) erhalten.

#### *4.4.1 DATENAUFBEWAHRUNGSRICHTLINIE*

Ihre Kundendaten werden im HubSpot-System gespeichert, solange Sie ein aktiver Kunde bei uns sind. Die HubSpot-Plattform bietet aktiven Kunden die entsprechenden Tools, um ihre Daten nach Belieben zu löschen. Daten ehemaliger Kunden werden auf schriftliche Anforderung des jeweiligen Kunden oder nach Ablauf einer vorgegebenen Frist nach Beendigung sämtlicher Verträge mit dem Kunden entfernt. Daten von Freemium-Kunden werden gelöscht, wenn das Portal nicht mehr aktiv genutzt wird. Daten ehemaliger zahlender Kunden werden 90 Tage nach Ende jeglicher Kundenbeziehungen von HubSpot gelöscht. In Replikaten, Snapshots und Sicherungskopien gespeicherte Daten werden nicht aktiv, sondern nach einer Zeit automatisch aus ihren Aufbewahrungsorten gelöscht, wenn das Ende des jeweiligen Datenzyklus erreicht ist. HubSpot speichert bestimmte Daten, wie Protokolle und dazugehörige Meta-Daten, um Sicherheits- und Compliance-Bestimmungen sowie gesetzliche Anforderungen einzuhalten.

#### *4.4.2 VERWALTUNG DES DATENSCHUTZPROGRAMMS*

Die Rechts- und Sicherheitsabteilung sowie diverse andere Teams von HubSpot arbeiten gemeinsam daran, die Effektivität und lückenlose Umsetzung unseres Datenschutzprogramms zu gewährleisten. Eine detailliertere Beschreibung unserer Verpflichtung zum Schutz Ihrer Daten finden Sie in unserer [Datenschutzrichtlinie](#) und in der [Vereinbarung zur Datenverarbeitung](#).

### **4.5 GESCHÄFTSKONTINUITÄT UND DISASTER RECOVERY**

HubSpot unterhält Geschäftskontinuitäts- und Disaster-Recovery-Pläne, deren Schwerpunkt jeweils auf der Vermeidung von Ausfällen durch die Redundanz von Telekommunikation, Systemen und Geschäftsbetrieb sowie auf Strategien zur schnellen Wiederherstellung im Falle von Verfügbarkeits- oder Leistungsbeeinträchtigungen liegt. Treten Umstände ein, die Auswirkungen auf unsere Kunden haben, so hat sich HubSpot zum Ziel gesetzt, das jeweilige Problem schnell und transparent zu isolieren und zu beheben. Erkannte Probleme werden auf der [Statusseite von HubSpot](#) veröffentlicht. Die Einträge werden anschließend laufend aktualisiert, bis das jeweilige Problem behoben ist.

#### *4.5.1 ZUVERLÄSSIGKEIT UND WIEDERHERSTELLUNG VON SYSTEMEN*

Geschäftskontinuitätstests werden im Rahmen der regulären Datenverarbeitung von HubSpot durchgeführt. Die Wiederherstellungsprozesse bei HubSpot werden laufend durch reguläre Wartungs- und Supportprozesse validiert. Gemäß dem Prinzip der kontinuierlichen Bereitstellung erstellen oder löschen wir täglich im Rahmen unserer regulären Wartungs- und Entwicklungsarbeiten zahlreiche Serverinstanzen. Außerdem verwenden wir diese Verfahren zur Wiederherstellung, falls es zu einer



Beeinträchtigung von Serverinstanzen und anderen Fehlern kommt. Unser Wiederherstellungsprozess gehört somit zur täglichen Routine.

HubSpot setzt primär auf Infrastruktur-Redundanz, Echtzeit-Replikation und Sicherungskopien. Alle HubSpot-Produktservices werden mit vollständiger Redundanz erstellt. Die Serverinfrastruktur wird strategisch auf mehrere separate Verfügbarkeitszonen und virtuelle private Cloud-Netzwerke innerhalb unseres Infrastrukturanbieters verteilt. Zudem werden alle Web-, Anwendungs- und Datenbankkomponenten mit mindestens n+1 unterstützenden Serverinstanzen oder Containern bereitgestellt.

#### 4.5.2 DATENSICHERUNGSSTRATEGIE

HubSpot stellt sicher, dass Daten repliziert und in mehreren dauerhaften Datenspeichern gesichert werden. Die Aufbewahrungsdauer von Sicherungskopien hängt von der Art der Daten ab. Darüber hinaus werden Daten über verschiedene Verfügbarkeitszonen und Infrastrukturstandorte hinweg repliziert, um für Fehlertoleranz sowie bei Bedarf für Skalierbarkeit und eine rasche Wiederherstellung zu sorgen.

- Im Rahmen der unmittelbaren Datensicherung werden Kunden- bzw. Endnutzerdaten durch Nutzung mehrfacher Online-Replikate gesichert. Alle Datenbanken der Produktionsebene verfügen zu jedem Zeitpunkt über je eine primäre Kopie (Master) und ein Replikat (Slave) der Live-Daten. Bei allen Datenbanken werden die Sicherungskopien der letzten sieben Tage jeweils so gespeichert, dass eine einfache Wiederherstellung sichergestellt ist. Snapshots werden mindestens einmal pro Tag erstellt und mittels eines zusätzlichen Dienstes aufbewahrt; falls möglich erfolgt eine Echtzeit-Replikation. Alle Daten der Produktionsebene werden in einem verteilten Dateisystem gespeichert, wie etwa Amazon S3.
- Da wir für Hosting-, Datensicherungs- und Wiederherstellungszwecke private Cloud-Lösungen verwenden, kommen HubSpot-Produkte gänzlich ohne physische Infrastrukturen bzw. Speichermedien aus. Im Rahmen der Bereitstellung der HubSpot-Produkte für Kunden werden darüber hinaus keinerlei Hardcopy-Medien (z. B. Papier, Klebefolie usw.) verwendet.
- Standardmäßig werden alle Sicherungskopien durch Zugriffsbeschränkungen der Produktinfrastruktur-Netzwerke von HubSpot, durch Zugriffssteuerungslisten für Dateisysteme, in denen die Datensicherungsdateien gespeichert werden, und/oder durch Datenbanksicherungsmaßnahmen geschützt.
- Kunden, die ihre Daten zusätzlich sichern möchten, finden in der HubSpot-Plattform zahlreiche verschiedene Möglichkeiten dafür. Viele der Funktionen in Ihrem HubSpot-Portal enthalten Exportoptionen und mithilfe der [HubSpot-Bibliothek öffentlicher APIs](#) können Sie Ihre Daten mit anderen Systemen synchronisieren. Ausführliche Informationen zum Sichern Ihrer Daten finden Sie in unserem [Wissensdatenbankartikel über das Exportieren Ihrer Inhalte](#).

## 4.6 UNTERNEHMENS SICHERHEIT BEI HUBSPOT

### 4.6.1 MITARBEITERAUTHENTIFIZIERUNG UND -AUTORISIERUNG



HubSpot verwendet unternehmensweit eine branchenübliche Kennwortrichtlinie. Diese Richtlinie schreibt eine Änderung von Kennwörtern in Intervallen von maximal 90 Tagen vor. Darüber hinaus müssen Kennwörter aus mindestens acht Zeichen und einer Kombination aus Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen bestehen. HubSpot gestattet keine gemeinsame Nutzung von Accounts und Kennwörtern durch Mitarbeiter.

In der Regel authentifizieren sich Mitarbeiter via SSH-Schlüssel für den Zugriff auf HubSpot-Produkte. Sofern Kennwörter gestattet sind, müssen diese gemäß der Kennwortrichtlinie 12 Zeichen umfassen. Überdies funktionieren alle Tools, auf denen unsere Produkte basieren, nach dem Prinzip der Multi-Faktor-Authentifizierung, oder sind durch Single-Sign-On-Lösungen geschützt, die Multi-Faktor-Authentifizierung nutzen.

#### **4.6.2 ZUGRIFFSVERWALTUNG**

HubSpot hat die Authentifizierungs- und Autorisierungsverfahren für den Mitarbeiterzugriff auf die HubSpot-Systeme reglementiert und automatisiert. Dies gilt auch für die Marketing- und Vertriebsplattformen. Alle Zugriffe werden protokolliert. In den meisten Fällen wird der Zugriff auf der Grundlage eines rollenbasierten Zugriffssteuerungsmodells gewährt. Der Just-in-Time-Zugriff (JITA) ist in die automatischen Verfahren mit einer Reihe strenger Autorisierungsmechanismen integriert.

Wir haben umfangreiche Supportsysteme entwickelt, um unser Sicherheitsmanagement und unsere Compliance-Aktivitäten zu optimieren und zu automatisieren. Neben zahlreichen weiteren Funktionen bereinigt das System unsere Produkt- und Firmeninfrastruktur mehrmals täglich, um zu gewährleisten, dass die geeigneten Berechtigungen gewährt werden, um Mitarbeiterereignisse zu verwalten, Konten und Zugänge bei Bedarf zu widerrufen, Protokolle mit Zugriffsanfragen zu erstellen und Compliance-Nachweise für jede unserer technologischen Sicherheitskontrollen zu erfassen. Diese internen Systeme bereinigen die Infrastruktur alle 24 Stunden und prüfen dabei, ob diese die genehmigten Konfigurationen erfüllt.

#### **4.6.3 HINTERGRUNDÜBERPRÜFUNGEN**

HubSpot-Mitarbeiter müssen eine ausführliche Hintergrundüberprüfung durch Dritte durchlaufen, sofern dies gemäß lokalen Vorschriften und Beschäftigungsstandards erlaubt ist, bevor ihnen ein formelles Stellenangebot unterbreitet werden kann. Im Vordergrund stehen dabei in erster Linie Informationen zu bisherigen beruflichen Tätigkeiten, dem Bildungsgrad sowie eventuellen Vorstrafen der Bewerber. Die Überprüfung möglicher Referenzen erfolgt nach Ermessen der Manager. Sämtliche Mitarbeiter müssen eine Vertraulichkeitsvereinbarung und Richtlinie zur akzeptablen Nutzung unterzeichnen, um auf Unternehmens- und Produktionsnetzwerke zugreifen zu dürfen.

#### **4.6.4 PHYSISCHE UNTERNEHMENS SICHERHEIT BEI HUBSPOT**

Die Niederlassungen von HubSpot sind mehrfach gesichert. An allen HubSpot-Niederlassungen weltweit gewährleisten Sicherheitskräfte ein sicheres Umfeld für HubSpot-Angestellte. Der Zugang wird mittels RFID-Token kontrolliert, die mit den Mitarbeitern verknüpft sind und automatisch deaktiviert werden, wenn sie nicht mehr gebraucht werden (z. B. bei Beendigung des Arbeitsverhältnisses, seltenem Gebrauch usw.). Darüber hinaus werden HubSpot-Niederlassungen mit Videoüberwachung und vielen weiteren Schutzvorkehrungen gesichert.



#### 4.6.5 ANBIETERMANAGEMENT

Wir nutzen eine kleine Zahl von externen Dienstleistern, die dafür sorgen, dass die HubSpot-Produkte die Marketing-, Vertriebs- und Serviceanforderungen unserer Kunden so gut wie möglich erfüllen. Wir betreiben ein Programm zum Anbietermanagement, um angemessene Sicherheits- und Datenschutzkontrollen zu gewährleisten. Das Programm umfasst Inventarisierung, Tracking und Überprüfung der Sicherheitsprogramme der Anbieter, die HubSpot unterstützen.

Geeignete Schutzmaßnahmen werden im Verhältnis zur jeweils erbrachten Dienstleistung und zur Art der ausgetauschten Daten bewertet. Eine lückenlose Einhaltung des erwarteten Schutzes wird im Rahmen unserer Vertragsbeziehung mit unseren Anbietern gesteuert. Unser Sicherheitsteam, unsere Rechtsabteilung und die Geschäftseinheit, die für den jeweiligen Vertrag zuständig ist, koordinieren individuelle Bedingungen für unsere Anbieter im Rahmen der Vertragsverwaltung.

#### 4.6.6 SICHERHEITSBEWUSSTSEIN UND SICHERHEITSRICHTLINIEN

Damit unser gesamtes technisches Personal, alle unsere Kundendienstmitarbeiter und sonstige Mitarbeiter im Hinblick auf den Schutz Ihrer Daten an einem Strang ziehen, hat HubSpot eine Sicherheitsrichtlinie für schriftliche Informationen entwickelt und pflegt diese beständig. Die Richtlinie enthält neben vielen weiteren Themen Anforderungen für die Datenverarbeitung, Datenschutzüberlegungen und Reaktionen auf Verstöße.

Mit dieser Richtlinie und den vielen verschiedenen eingerichteten Schutzmaßnahmen und -standards gewährleisten wir überdies, dass die HubSpot-Mitarbeiter sorgfältig für ihre Aufgaben geschult sind. HubSpot-Mitarbeiter durchlaufen ein mehrstufiges Sicherheitstraining, das auf ihre Rolle und die damit verbundenen Zugriffsrechte zugeschnitten ist. Alle neu eingestellten Mitarbeiter durchlaufen eine allgemeine Schulung zum Sicherheitsbewusstsein. Darin werden unter anderem die Sicherheitsvorschriften von HubSpot behandelt. Nach der ersten Schulung stehen unterschiedliche Weiterbildungspfade zur Verfügung, je nach der Rolle eines Mitarbeiters. Entwicklerspezifische Schulungen werden von den Entwicklerteams bei HubSpot angeboten und gestaltet. Funktionsspezifische Schulungen für mehr Sicherheitsbewusstsein werden für Services & Support, Sales und viele andere Funktionen angeboten und auf die individuellen Umstände der jeweiligen Funktion zugeschnitten. Über regelmäßige Updates, Mitteilungen und interne Veröffentlichungen können Mitarbeiter ihre Kenntnisse zum Thema Sicherheit immer wieder auffrischen.

### 4.7 VORFALLMANAGEMENT

HubSpot ist das ganze Jahr über rund um die Uhr erreichbar, um schnell auf sämtliche Vorfälle, die die Sicherheit oder den Datenschutz betreffen, reagieren zu können. Das HubSpot-Programm für schnelle Reaktion auf Störfälle gewährleistet in solchen Fällen ein schnelles, zuverlässiges Eingreifen. Vordefinierte Vorfällttypen werden auf der Basis von historischen Trendanalysen erstellt, um ein zeitnahes Tracking von Vorfällen sowie eine einheitliche Aufgabenzuweisung, Weiterleitung und Kommunikation zu gewährleisten. Viele automatisierte Prozesse fließen in den Reaktionsprozess für Vorfälle ein, einschließlich Warnungen bei böswilligen Aktivitäten oder Anomalien, Warnungen an Anbieter, Reaktionen auf Kundenanfragen, Warnungen bei Datenschutzvorfälle usw.



Bei der Reaktion auf einen Vorfall ermitteln wir zuerst das Risiko für die von HubSpot verwalteten Informationen sowie die Quelle des Problems, soweit möglich. Wir melden uns per E-Mail oder telefonisch (sofern die E-Mail-Kommunikation nicht ausreicht) beim jeweiligen Kunden (und etwaigen weiteren betroffenen Kunden). Wir bieten je nach Bedarf regelmäßige Updates, um eine angemessene Lösung des Vorfalls zu gewährleisten.

Unser Chief Security Officer überprüft jegliche vermuteten oder bestätigten Sicherheitsvorfälle. Je nach Art des Vorfalls wird unter Einsatz der geeigneten Mittel und in Rücksprache mit den betroffenen Kunden eine angemessene Lösung ausgearbeitet.

## 5 PRODUKTSICHERHEITSFUNKTIONEN

Das Sicherheitsprogramm von HubSpot wurde entwickelt, um die Sicherheit unserer gesamten Produktpalette zu gewährleisten. Jedes unserer Produkte basiert auf Sicherheitsverfahren für die Entwicklung von Anwendungen und wird durch Infrastruktursicherheit und Konfigurationen für eine hohe Verfügbarkeit geschützt.

Unabhängig davon, ob Sie ein kostenloses oder kostenpflichtiges HubSpot-Produkt mit vielen oder wenigen Funktionen nutzen, sind wir bestrebt, Ihnen den bestmöglichen Datenschutz zu bieten. Daten, die Sie in HubSpot-Produkten speichern, gehören Ihnen. Unser Sicherheitsprogramm wurde entwickelt, um Ihre Daten zu schützen und diese werden von uns ausschließlich zur Bereitstellung der HubSpot-Dienste genutzt. Ihre Daten werden von HubSpot nicht mit anderen Kunden geteilt oder weiterverkauft.

### 5.1 MARKETING HUB

Info: Marketing Hub ist branchenweit führend unter den Lösungen für Marketing-Automatisierung. Die Lösung bietet Ihnen anwenderfreundliche und effektive Tools zur Verwaltung Ihrer Inbound-Marketing-Strategie.

Hosting: Die primäre Content-Management-System (CMS)-Infrastruktur wird auf Amazon Web Services und Google Cloud Platform gehostet. Die Hosting-Strategie von HubSpot gewährleistet zusätzliche Redundanzen, Flexibilität bei der Systemarchitektur und Reaktionsfähigkeit der Infrastruktur. Unsere Implementierungsabläufe basieren auf den oben beschriebenen Netzwerk- und Serversicherheitsstandards und Verfügbarkeitsfunktionen.

Web Application Firewall (WAF): Auf HubSpot-Produkten gehostete Kunden-Websites werden von unserer branchenführenden Web Application Firewall. Ihre auf HubSpot gehosteten Websites, Blogs, Landing-Pages und sonstigen Online-Präsenzen werden standardmäßig vor den neuesten Distributed Denial-of-Service (DDoS)-Angriffen und sonstigen Bedrohungen für Webanwendungen geschützt. Wenn Sicherheitsvorfälle auftreten, handeln das Security-Operations- und das DevOps-Team von HubSpot unverzüglich, um sicherzustellen, dass Ihre Websites durchgehend rund um die Uhr geschützt bleiben.

Transport Layer Security (TLS): Für Nutzer von Marketing Hub besteht die Möglichkeit, TLS-Dienste für ihre Websites, Landing-Pages und Analytics-Daten zu Besucherinteraktionen zu aktivieren. Standardmäßig verwenden TLS-Zertifikate Subject Alternative Names und werden von unserem



Content-Delivery-Anbieter verwaltet. Weitere Informationen zu ersten Schritten finden Sie in [diesem Artikel](#).

Verschlüsselungsoptionen: Kunden-Websites, die HTTPS verwenden, werden standardmäßig für die Unterstützung von TLS 1.0, 1.1, 1.2 und 1.3 konfiguriert. Es ist jedoch möglich, die Unterstützung für eines oder mehrere dieser Protokolle zu deaktivieren. Kunden können für ihre von HubSpot gehostete Domain auch HTTP Strict Transport Security (HSTS) aktivieren. Wenden Sie sich diesbezüglich bitte an den HubSpot-Support oder Ihren Customer Success Manager.

## 5.2 HUBSPOT CRM

Info: Das HubSpot CRM ist nur eines der zahlreichen Produkte von HubSpot, von denen Ihr Vertriebsteam begeistert sein wird. Wenn Sie in der Vertriebsbranche tätig sind, können Sie die leicht zu bedienende Anwendung kostenlos nutzen. Der Einstieg in das HubSpot CRM nimmt nur wenige Minuten in Anspruch. Gehen Sie dazu zur [CRM-Produktseite von HubSpot](#).

Sicherheit als Standard („Secure by default“): Das HubSpot CRM unterliegt denselben Sicherheitsmaßnahmen wie alle anderen HubSpot-Produkte. Die Anwendung wurde auf Basis unserer langjährigen Erfahrung in den Bereichen einer fortgeschrittenen, sicheren Softwareentwicklung sowie der Verwaltung von Infrastruktur und Fehlermeldesystemen entwickelt.

E-Mail-Integrationen und verknüpftes E-Mail-Konto: Als CRM-Benutzer haben Sie die Möglichkeit, Ihr Gmail-, Office365- oder IMAP-fähiges E-Mail-Konto mit dem System zu verknüpfen. Gmail- und Office365-Integrationen werden durch die nativen Integrationsfunktionen in diesen Plattformen autorisiert und geschützt. Durch die IMAP-Integration kann Ihr verknüpftes E-Mail-Konto E-Mail-Nachrichten aus anderen E-Mail-Diensten mit Ihrem CRM synchronisieren. Wenn ein Benutzer eine IMAP-Integration einrichtet, wird das HubSpot-Produkt entsprechend als IMAP-Client genutzt. Die Dienste, die IMAP-Integrationen unterstützen, umfassen zahlreiche integrierte Schutzmechanismen: Die Daten werden bei der Übermittlung durchgängig geschützt. Die Daten im Speicher werden auf Feld- und auf Datenbankebene verschlüsselt. Die Zugriffssteuerungen sorgen dafür, dass nur berechtigte Benutzer auf die Daten zugreifen können.

Datenschutz: Unabhängig davon, ob Sie ein kostenloses oder kostenpflichtiges HubSpot-Produkt nutzen, sind wir stets bestrebt, Ihnen den bestmöglichen Datenschutz zu bieten. Daten, die Sie in HubSpot-Produkten speichern, gehören Ihnen. Die Daten werden von uns ausschließlich zur Bereitstellung der Dienste genutzt.

Hosting: Die CRM-Infrastruktur wird auf Amazon Web Services gehostet und nutzt dieselbe Infrastruktur-Redundanz und -Flexibilität wie die restliche HubSpot-Infrastruktur. Unsere Hosting-Strategie trägt überdies zur Gewährleistung einer erstklassigen Infrastruktur und Netzwerksicherheit und -verfügbarkeit bei.

Zugriffssteuerung: Das HubSpot CRM verfügt über ein benutzerfreundliches und intuitives Rollenzuweisungssystem, mit dem Sie einzelnen Mitarbeitern Ihres Vertriebsteams die entsprechenden Zugangsberechtigungen erteilen können. Weitere Informationen finden Sie in diesem [Hilfeartikel zu Benutzerrollen](#).

## 5.3 SALES HUB



Info: Die Sales Hub-Produkte enthalten spezialisierte Tools für den Vertrieb, die es Vertriebsmitarbeitern ermöglichen, gezielter mit ihren Leads zu interagieren und ihre Konversionsraten zu verbessern.

Hosting: Die grundlegende Back-End-Infrastruktur von Sales Hub wird auf Amazon Web Services gehostet. Dabei wird dieselbe Infrastruktur-Redundanz und -Flexibilität wie bei der übrigen HubSpot-Infrastruktur verwendet.

Datenspeicherung: Sales Hub speichert E-Mail-Metadaten, um E-Mail-Tracking, Link-Wrapping und Connections-Dienste zu ermöglichen. Daten werden in geschützten Speichern innerhalb der HubSpot-Infrastruktur aufbewahrt. Der Zugriff auf diese Daten wird strengstens kontrolliert. Lediglich einige wenige Mitarbeiter haben je nach ihrer Rolle Zugriff auf die Datenspeicher. Dies gilt für Mitarbeiter, die auf die Daten zugreifen müssen, um Kundensupport- und ähnliche Anfragen zu beantworten.

Reibungslose Aktualisierung: Die Sales-Tools wurden entwickelt, um Vertriebsprozesse produktiver zu gestalten. In diesem Sinne wird z. B. die E-Mail-Erweiterung von HubSpot automatisch aktualisiert. Updates werden automatisch heruntergeladen und installiert, damit Sie nicht laufend Benachrichtigungen erhalten, die Sie daran erinnern sollen, ein Update vorzunehmen.

## 5.4 SERVICE HUB

Info: Service Hub enthält alle Funktionen, die Sie für zufriedene Kunden brauchen. Mit Service Hub haben Sie die Möglichkeit, Gespräche nahtlos nachzuverfolgen, und können Besuchern innovative Bot-Technologie bieten.

Hosting: Die grundlegende Back-End-Infrastruktur von Service Hub wird auf Amazon Web Services gehostet. Dabei wird dieselbe Infrastruktur-Redundanz und -Flexibilität wie bei der übrigen HubSpot-Infrastruktur verwendet.

Reibungslose Aktualisierung: Service Hub-Tools wurden entwickelt, um stets eine positive Nutzererfahrung der Kunden mit den angebotenen Services zu gewährleisten. Service Hub-Tools werden in regelmäßigen Abständen automatisch aktualisiert, damit die angebotenen Funktionen stets den wachsenden Anforderungen von Kunden an den Kundenservice entsprechen.

## 6 COMPLIANCE

HubSpot ist Inhaber eines [TRUSTe-Zertifikats für Unternehmensdatenschutz](#) und erfüllt die Bedingungen des [EU-US Privacy Shield](#). Außerdem enthält die HubSpot-Plattform praktische Funktionen, mit denen unsere Kunden ihre Anforderungen hinsichtlich DSGVO-Compliance mühelos erfüllen können. Ausführliche Informationen zur Einhaltung von Datenschutzvorschriften bei der Nutzung von HubSpot-Produkten finden Sie in unseren [Ausführungen zur DSGVO-Compliance](#) und in der [Vereinbarung zur Datenverarbeitung von HubSpot](#).

Die Produkte von HubSpot werden über erstklassige Cloud-Infrastrukturanbieter angeboten, darunter [Amazon Web Services](#) und [Google Cloud Platform](#). Die HubSpot-Infrastrukturanbieter verfügen über



SOC 2 Typ II- sowie ISO 27001-Zertifizierungen und schützen Einrichtungen vor elektronischen und physischen Angriffen.

## 7 UMFANG UND VERWENDUNG DIESES DOKUMENTS

Wir legen hinsichtlich der Bereitstellung unserer Lösungen für unsere Kunden Wert auf Transparenz. Dieses Dokument wurde im Hinblick auf unser Transparenzversprechen verfasst. Wir verbessern unsere Sicherheits- und Schutzmaßnahmen fortlaufend. Im Zuge dieser Bemühungen dienen die in diesem Dokument enthaltenen Informationen und Daten (sowie jegliche zugehörigen Kommunikationen) nicht dem Zweck, vertragliche Verpflichtungen jeglicher Art zwischen HubSpot und Dritten festzulegen oder bestehende Abkommen zu ändern, zu ergänzen oder zu überarbeiten.