Letzte Aktualisierung: Oktober 2021

Sicherheit im Überblick

HubSpot

Inhaltsverzeichnis

HubSpot: Sicherheit im Überblick

Unser Unternehmen und unsere Produkte

HubSpot ist die weltweit führende Plattform für Inbound-Marketing, Vertrieb, Kundenservice, Content-Management und Operations. Bereits seit 2006 stellt HubSpot umfassende Lösungen für Marketing, Vertrieb und Kundenservice bereit. Inzwischen nutzen über 120.000 Unternehmen in mehr als 120 Ländern HubSpots preisgekrönte Software sowie die Service- und Supportangebote des Unternehmens, um die Art und Weise zu optimieren, wie sie mit ihren Kundinnen und Kunden interagieren.

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

Sicherheit und Risikofokus bei HubSpot

Im Mittelpunkt der Sicherheitsstrategie von HubSpot steht der Schutz von Kundendaten. Aus diesem Grund hat HubSpot in geeignete Ressourcen und Kontrollverfahren investiert, die gewährleisten, dass wir unseren Kundinnen und Kunden einen hochwertigen und vor allem sicheren Service bieten können. In diesem Zusammenhang wurden auch ein spezielles Unternehmens- sowie ein Produktsicherheitsteam 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 Information Security Officer ist für die Implementierung von Sicherheits- und Schutzmaßnahmen bei HubSpot und allen dazugehörigen Produkten zuständig.

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 Kundinnen und 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 Kundinnen und Kunden eine ständige Verfügbarkeit von Diensten und Daten. Zudem arbeiten wir proaktiv an der Minimierung jeglicher Sicherheitsrisiken, die Serviceunterbrechungen bedingen könnten.
- Informations- und Serviceintegrität: Wir stellen sicher, dass die Daten unserer Kundinnen und Kunden weder korrumpiert noch in unangemessener Weise verändert werden.
- Einhaltung von Standards: Wir haben unser Sicherheitsprogramm anhand der branchenüblichen Richtlinien und bewährten Praktiken für Cybersicherheit erstellt, einschließlich der Critical Security Controls des Center for Internet Security (CIS). Unsere Kontrollmechanismen rund um die Verfügbarkeit, Vertraulichkeit und Sicherheit von Kundendaten sind außerdem so konzipiert, dass sie den SOC 2-Prinzipien (Trust Service Principles, TSPs) des American Institute of Certified Public Accountants (AICPA) entsprechen.

Sicherheitsmechanismen von HubSpot

Um die uns anvertrauten Daten zu schützen, verfolgt HubSpot einen „Defense-in-Depth"-Ansatz, um mehrere Ebenen von Sicherheitskontrollen im gesamten Unternehmen zu implementieren. In den folgenden Abschnitten werden einige der Kontrollmechanismen beschrieben, zu denen wir häufig Fragen erhalten.

Produktinfrastruktur von HubSpot

Sicherheit der Cloud-Infrastruktur

HubSpot hostet keine Produktsysteme an seinen eigenen Unternehmensstandorten. Die Produktinfrastruktur von HubSpot wird bei führenden Anbietern für Cloud-Infrastrukturen gehostet – z. B. Amazon Web Services (AWS). Unsere Hosting-Anbieter garantieren eine Serviceverfügbarkeit zwischen 99,95 % und 100 % und gewährleisten eine Redundanz aller Stromversorgungs-, Netzwerk- und Heizungs-/Klimaanlagendienste.

Die AWS-Produktinfrastruktur von HubSpot befindet sich im Osten der USA. Beide Anbieter verfügen über ein geprüftes Sicherheitsprogramm sowie über physische, umfeldbedingte und infrastrukturelle Sicherheitsvorkehrungen. Die Pläne für Geschäftskontinuität und Notfallwiederherstellung wurden im Rahmen der Zertifizierungen nach SOC 2 Typ II und ISO 27001 unabhängig geprüft.

Die Compliance-Dokumentation ist auf der Cloud-Compliance-Seite von AWS öffentlich zugänglich.

HubSpot stellt Ihnen auch einen Artikel in der Wissensdatenbank zur Verfügung, der häufig gestellte Fragen zu unserer Cloud-Infrastruktur beantwortet: Sie finden ihn hier.

Netzwerksicherheit und Perimeterschutz

Die HubSpot-Produktinfrastruktur erzwingt eine mehrschichtige Filterung und Prüfung aller Verknüpfungspunkte innerhalb der Plattform.

Es wurden Zugangskontrolllisten auf Netzwerkebene implementiert, um einen unbefugten Netzwerkzugriff auf unsere interne Produktinfrastruktur zu verhindern. Die Firewalls sind so

konfiguriert, dass Netzwerkverbindungen, die nicht ausdrücklich zugelassen sind, standardmäßig abgelehnt werden. Der Datenverkehr wird überwacht, um anormale Aktivitäten zu erkennen.

Änderungen unserer Netzsicherheit werden aktiv überwacht und durch standardisierte Änderungskontrollverfahren kontrolliert. Die Firewall-Regeln werden jährlich überprüft, um sicherzustellen, dass nur notwendige Verbindungen konfiguriert werden.

Konfigurationsmanagement

Durch Automatisierung sind wir in der Lage, unsere Vorkehrungen entsprechend den Anforderungen unserer Kundinnen und Kunden zu skalieren. Die Produktinfrastruktur ist eine hochautomatisierte Umgebung, in der die Kapazitäten und Fähigkeiten nach Bedarf erweitert werden können. Die Serverinstanzen werden von der Inbetriebnahme bis zur Ausrangierung streng kontrolliert, um sicherzustellen, dass Abweichungen von den Konfigurationsstandards erkannt und in einem vordefinierten Zeitraum rückgängig gemacht werden. Falls ein Produktionsserver von der Standardkonfiguration abweicht, wird er innerhalb von 30 Minuten mit der Standardkonfiguration überschrieben.

Alle Konfigurationen des Servertyps sind in Bilder und 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 erfolgt mit automatisierten Konfigurationsmanagement-Tools oder durch das Entfernen von Serverinstanzen, die nicht mehr mit dem erwarteten Standard konform sind, und der Bereitstellung einer Ersatzinstanz an ihrer Stelle. Unsere täglichen Infrastrukturprozesse beinhalten eine rigorose und automatisierte Konfigurationsverwaltung.

Alarmierung und Monitoring

Bei HubSpot sind die Server-Erstellungsverfahren komplett automatisiert. Zusätzlich investieren wir intensiv in Technologien für automatische Überwachung, Alarmierung und Reaktionsfähigkeit, um potenzielle Probleme kontinuierlich zu beheben. Die

Produktinfrastruktur von HubSpot ist so konzipiert, dass Technik- und Administratorenteams 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 sowie das Problem untersuchen und beheben können. Beim Auftreten von unerwarteten oder böswilligen Aktivitäten werden die entsprechenden Fachkräfte automatisch benachrichtigt, um zu gewährleisten, dass Probleme rasch behoben werden können.

Zudem sind viele automatisierte Trigger in das System eingebaut, um auf unerwartete 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.

Schutz von Anwendungen

Bedrohungsabwehr bei Web-Anwendungen

Alle Kundeninhalte, die auf der Plattform gehostet werden, sind durch eine Web Application Firewall (WAF) geschützt. Die WAF ist auf Basis einer Kombination aus branchenüblichen und benutzerdefinierten Regeln konfiguriert, die automatisch die richtigen Sicherheitsfunktionen für einen optimalen Schutz unserer Kundinnen und 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.

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) besonders in den OWASP Top 10 und vergleichbaren Empfehlungen dokumentiert sind. Auch Schutzmaßnahmen gegen DDoS-Angriffe (Distributed Denial of Service) wurden eingerichtet. Diese tragen dazu bei, dass die Websites der Kundinnen und Kunden und andere Teile der HubSpot-Produkte durchgehend verfügbar sind.

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 werden unsere Produkte fortlaufend optimiert.

Jeden Tag werden Tausende Erweiterungen des Programmcodes vorgeschlagen, genehmigt, zusammengeführt und bereitgestellt. Vor der Bereitstellung wird der Code überprüft, getestet (falls zutreffend) und die Zusammenführung genehmigt. Genehmigungen werden von den Verantwortlichen für die jeweiligen Repositorys kontrolliert. Nachdem der Code genehmigt wurde, wird er automatisch an die kontinuierliche Integrationsumgebung von HubSpot übermittelt. Dort erfolgen Kompilierung, Bündelung und Tests.

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.

Wir nutzen extensives Software-Gating und Traffic-Management, um Funktionen je nach den Vorlieben der Kundinnen und Kunden zu steuern (private Beta-Version, öffentliche Beta-Version, Veröffentlichung). HubSpot bietet nahtlose Updates. Da es sich um eine SaaS-Anwendung handelt, gibt es keine Ausfallzeiten im Zusammenhang mit Versionsveröffentlichungen. Wesentliche Änderungen an den Funktionen werden entweder über In-App-Benachrichtigungen und/oder Beiträge zu Produkt-Updates (auf Englisch) 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 Zugriff von der Qualitätssicherungs- oder Produktionsumgebung aus.

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.

Schwachstellen-Scans sind so konfiguriert, dass täglich nach nutzbaren Schwachstellen gesucht wird. Kontinuierlich laufende Scans, die Verwendung adaptiver Scan-Aufnahmelisten und die ständige Aktualisierung von Schwachstellen-Signaturen unterstützen HubSpot als präventive Maßnahmen gegen viele Sicherheitsbedrohungen.

Außerdem führen wir gemeinsam mit branchenweit anerkannten Dritten jährliche Penetrationstests durch. 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.

Neben internen Schwachstellen-Scans und Penetrationstests durch Dritte verwaltet HubSpot ein Bug-Bounty-Programm, bei dem unabhängige Sicherheitsexperten eingeladen werden, an der Identifizierung von Sicherheitslücken in den HubSpot-Produkten teilzunehmen. Sicherheitstests von Testportalen durch Mitglieder der Security-Community und HubSpot-Kundinnen und -Kunden werden ausdrücklich begrüßt. Informationen über das Bug-Bounty-Programm von HubSpot finden Sie unter https://bugcrowd.com/hubspot (auf Englisch).

Schutz von Kundendaten

Logische Trennung von Mandantendaten

HubSpot bietet eine hochgradig skalierbare, mehrmandantenfähige SaaS-Lösung. Die HubSpot-Benutzerfläche und unsere APIs beschränken den Zugriff ausschließlich auf autorisierte Inhalte. HubSpot segmentiert die Daten logisch mithilfe von Portal-IDs und verknüpft jede eindeutige ID mit allen Daten und Objekten der einzelnen Kundinnen und Kunden. Die Informationen werden über die Benutzeroberfläche oder die für ein

bestimmtes HubSpot-Portal zu erstellenden APIs zur Verfügung gestellt, ohne dass die Gefahr eines portalübergreifenden Zugriffs oder einer Verunreinigung von Daten besteht.

Autorisierungsregeln werden in das Design integriert und laufend geprüft. Außerdem protokollieren wir die Anwendungsauthentifizierung und die damit verbundenen Änderungen, die Verfügbarkeit der Anwendung und die Seitenaufrufe der Benutzerinnen und Benutzer.

Vertrauliche Informationen

Die HubSpot-Produkte bieten ein integriertes Kundenerlebnis für Marketing-, Vertriebs-, Kundenservice-, Content-Management- und Operations-Teams. Bei den von uns erfassten Daten handelt es sich um Informationen, die aus Interaktionen mit Interessentinnen und Interessenten bzw. Kundinnen und Kunden, öffentlichen Verzeichnissen und anderweitigen vertrauenswürdigen Quellen stammen.

Die HubSpot-Tools ermöglichen es Kundinnen und Kunden, selbst festzulegen, welche Daten erfasst und für sie gespeichert werden sollen. Gemäß den Nutzungsbedingungen von HubSpot und der Richtlinie zur akzeptablen Nutzung sind unsere Kundinnen und Kunden dafür verantwortlich, nur Daten zu erfassen, die zur Förderung ihrer Marketing-, Vertriebs-, Service-, Content-Management- und Operations-Prozesse angemessen sind. Die HubSpot-Produkte sollten nicht zur Erfassung sensibler Daten wie Kredit- oder Bankkartennummern, Informationen zu privaten Bankkonten, Sozialversicherungsnummern, Reisepassnummern, Führerscheinnummern, Finanzauskünften oder Daten zur Beschäftigung oder Gesundheit eingesetzt werden.

Weitere Informationen über die Klassifizierung der von HubSpot verwendeten und unterstützten Daten finden Sie in der Tabelle zur Datenklassifizierung in unserem SOC 2-Bericht.

Verschlüsselung bei der Übermittlung und im Speicher

Sämtliche sensiblen Interaktionen mit den HubSpot-Produkten (z. B. API-Aufrufe, authentifizierte Sitzungen usw.) werden bei der Übermittlung mit den TLS-Versionen 1.2 oder 1.3 und mindestens 2.048-Bit-Schlüsseln verschlüsselt. Transport Layer Security (TLS) ist auch der Standard für Kundinnen und Kunden, die ihre Websites auf der HubSpot-Plattform hosten.

Weitere Informationen zur Konfiguration von TLS finden Sie in unserem Leitfaden zur Einrichtung von Websites und in unserem Artikel in der Wissensdatenbank über SSL und Domain-Sicherheit.

Bei HubSpot werden verschiedene Technologien eingesetzt, um die Verschlüsselung von Daten im Speicher zu gewährleisten. Die Plattformdaten werden mit einer AES-256-Verschlüsselung gespeichert. Die Benutzerpasswörter werden den bewährten Praktiken der Branche entsprechend gehasht und verschlüsselt gespeichert. Bestimmte E-Mail-Funktionen verschlüsseln Nachrichtendaten sowohl im Speicher als auch bei der Übermittlung.

Schlüsselverwaltung

Schlüssel 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 Häufigkeit der Schlüsselrotation hängt von der Sensibilität der zu verschlüsselnden Daten ab. Im Allgemeinen werden TLS-Zertifikate jährlich erneuert.

HubSpot ist derzeit nicht in der Lage, von Kundinnen und Kunden bereitgestellte Verschlüsselungsschlüssel zu verwenden.

Datensicherung und Notfallplan

Zuverlässigkeit und Wiederherstellung von Systemen

HubSpot unternimmt alle wirtschaftlich angemessenen Anstrengungen, um die Verfügbarkeit unserer Systeme sicherzustellen und jeden Monat eine Serviceverfügbarkeit von 99,95 % für unseren Abonnementdienst zu erreichen. Lesen Sie bitte Abschnitt 7 der produktspezifischen Klauseln für weitere Informationen.

Darüber hinaus finden Sie auf der Statusseite von HubSpot Updates in Echtzeit und Verlaufsdaten zum Systemstatus und zur Sicherheit (auf Englisch).

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.

Notfallplan

HubSpot verfügt über einen Notfallwiederherstellungsplan, der jährlich im Rahmen unserer SOC 2-Kontrollen getestet wird. Weitere Einzelheiten entnehmen Sie bitte unserem SOC 2-Bericht (herunterladbar auf hubspot.de/security).

Datensicherungsstrategie

SYSTEMSICHERUNGEN

Die Systeme werden nach festgelegten Zeitplänen und in regelmäßigen Abständen gesichert. Bei allen Datenbanken werden die Sicherungskopien der letzten sieben Tage jeweils so gespeichert, dass eine einfache Wiederherstellung möglich ist. Die Sicherungen werden auf ihre erfolgreiche Ausführung hin überwacht. Bei Zwischenfällen werden Warnmeldungen generiert. Fehlermeldungen werden eskaliert, untersucht und behoben.

Die Daten werden täglich in der zugeordneten Region gesichert. Außerdem werden die Sicherungen regelmäßig in eine andere AWS-Region kopiert, um bei einem Ausfall der primären Region eine Wiederherstellung zu ermöglichen. Bei Wiederherstellungsfehlern werden Überwachungs- und Warnmeldungen ausgegeben und entsprechend eingestuft.

Alle Daten der Produktionsebene werden in einem hochverfügbaren Dateisystem gespeichert, wie etwa Amazon S3.

PHYSISCHER SICHERUNGSSPEICHER

Da wir für Hosting-, Datensicherungs- und Wiederherstellungszwecke öffentliche Cloud-Lösungen verwenden, kommen HubSpot-Produkte gänzlich ohne physische Infrastrukturen bzw. Speichermedien aus. Im Rahmen der Bereitstellung der HubSpot-Produkte für unsere Kundschaft werden keinerlei Hardcopy-Medien (z. B. Papier, Magnetband usw.) verwendet.

SCHUTZMASSNAHMEN FÜR SICHERUNGSKOPIEN

Standardmäßig werden alle Sicherungskopien durch Zugriffsbeschränkungen der Produktinfrastruktur-Netzwerke von HubSpot und durch Zugriffssteuerungslisten für Dateisysteme, in denen die Datensicherungsdateien gespeichert werden, geschützt.

SICHERUNGSOPTIONEN FÜR KUNDINNEN UND KUNDEN

Kundinnen und Kunden, die ihre Daten zusätzlich sichern möchten, finden auf 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.

Identitäts- und Zugangskontrolle

Produkt-Benutzerverwaltung

Die HubSpot-Produkte ermöglichen detaillierte Autorisierungsregeln. Kundinnen und Kunden können selbst die Benutzerinnen und Benutzer ihrer Portale erstellen und verwalten, die für ihre Accounts geeigneten Berechtigungen zuweisen und den Zugriff auf ihre Datenfunktionen beschränken.

Weitere Informationen zu Benutzerrollen finden Sie im Leitfaden für Benutzerrollen und -berechtigungen in HubSpot.

Schutzmaßnahmen bei der Anmeldung

Die HubSpot-Produkte ermöglichen es Benutzerinnen und 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. Benutzerinnen und Benutzer, die die integrierte HubSpot-Anmeldung verwenden, können die Standard-Kennwortrichtlinie nicht ändern.

Die Funktion „Mit Google anmelden“ steht allen HubSpot-Kundinnen und -Kunden zur Verfügung. Ein fortschrittlicheres SAML-basiertes SSO, das in jedes SAML-basierte IDP integriert ist, ist in jedem Hub mit Enterprise-Tarif verfügbar.

Kundinnen und Kunden, die einen SSO-Anbieter nutzen, können eine SSO-basierte Anmeldung für ihre Benutzerinnen und Benutzer einrichten. Anleitungen zum Einrichten von SSO finden Sie in diesem Artikel in der Wissensdatenbank sowie in der HubSpot Academy. Benutzerinnen und Benutzer, die sich mittels Single-Sign-On oder über Google anmelden, können bei ihrem SSO-Anbieter oder in ihren Google-Konten eigene Kennwortrichtlinien konfigurieren.

Kundinnen und Kunden, die die integrierte HubSpot-Anmeldung nutzen, wird empfohlen, eine zweistufige Authentifizierung für ihre HubSpot-Accounts einzurichten. Darüber hinaus können Portaladministratorinnen und Portaladministratoren über die Konfiguration ihrer HubSpot-Portale sicherstellen, dass die zweistufige Authentifizierung bei allen Benutzerinnen und Benutzern aktiviert ist.

Produkt-API-Autorisierung

Der Zugriff auf die Programmierschnittstelle (API) ist entweder über API-Schlüssel- oder OAuth (Version 2)-Autorisierung möglich. Kundinnen und 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 auf der HubSpot-Website vorgestellt werden. Die Autorisierung von OAuth-fähigen Anforderungen erfolgt im Rahmen festgelegter Umfänge. Weitere Informationen zur API-Nutzung finden Sie im Entwicklerportal auf HubSpot.com (auf Englisch).

Zugriff auf die Produktionsinfrastruktur

Der Zugriff auf die Systeme von HubSpot wird streng kontrolliert und folgt dem Prinzip der geringsten notwendigen Berechtigung. HubSpot-Mitarbeitenden wird der Zugriff mithilfe eines rollenbasierten Zugriffssteuerungsmodells (RBAC) gewährt.

Der tägliche Zugang ist auf jene Personen beschränkt, die ihn für ihre Tätigkeit benötigen. Für den Notfallzugriff (z. B. Fehlerbehebung oder Reaktionen auf Warnmeldungen) und den

Zugriff auf Verwaltungsfunktionen verwendet das HubSpot-System ein JITA-Modell (Just In Time Access), bei dem Benutzerinnen und Benutzer den Zugriff auf berechtigungsbasierte Funktionen für eine begrenzte Dauer beantragen können. Jeder JITA-Antrag wird protokolliert. Protokolle werden kontinuierlich auf anomale Anfragen hin überwacht. Nach Ablauf des konfigurierten Sitzungslimits läuft der Zugriff auf den Account ab und wird automatisch widerrufen.

Darüber hinaus sind direkte Netzwerkverbindungen zu Produktinfrastruktur-Geräten über SSH oder ähnliche Protokolle verboten. Entwicklungs- und Technikteams 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.

Der Zugriff von Mitarbeitenden auf Unternehmens- und Produktressourcen wird protokolliert. Es erfolgt eine tägliche automatisierte Überprüfung und eine mindestens halbjährliche Neuzertifizierung.

Zugriff auf Kundenportale durch Mitarbeitende von HubSpot

Mitarbeitende, die im Kundensupport, in Service-Teams oder in sonstiger Weise in der Kundenbetreuung tätig sind, können die JITA-Authentifizierung für einen begrenzten Zeitraum für den Zugriff auf Kundenportale anfordern. Zugriffsanträge sind auf die Aufgaben der Mitarbeitenden im Rahmen ihrer Support- und Kundenserviceverpflichtungen beschränkt. Die Anträge sind auf das Portal einer bestimmten Kundin bzw. eines bestimmten Kunden und einen Zeitraum von maximal 24 Stunden beschränkt. Alle Zugriffsanträge, Anmeldungen, Anfragen, Seitenaufrufe und ähnliche Informationen werden protokolliert.

Unternehmensauthentifizierung und -autorisierung

Der Zugriff auf das Unternehmensnetzwerk erfordert sowohl aus der Ferne als auch im Büro eine Multi-Faktor-Authentifizierung (MFA). Alle SaaS-Anwendungen, die von HubSpot verwendet werden, erfordern SSO mit MFA für eine zentralisierte Zugangskontrolle.

Die Passwortrichtlinien entsprechen den bewährten Praktiken der Branche, was die erforderliche Länge, Komplexität und Änderungsfrequenz betrifft.

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.

Unternehmenssicherheit bei HubSpot

Hintergrundüberprüfungen und Onboarding

HubSpot-Mitarbeitende in den USA müssen eine ausführliche Hintergrundüberprüfung durch Dritte durchlaufen, bevor ihnen ein formelles Stellenangebot unterbreitet werden kann. Im Fokus stehen dabei in erster Linie Informationen zu bisherigen beruflichen Tätigkeiten, dem Bildungsgrad sowie eventuellen Vorstrafen der Bewerberinnen und Bewerber. Außerhalb der USA werden frühere Arbeitsverhältnisse überprüft. Die Überprüfung möglicher Referenzen erfolgt nach Ermessen der für die Einstellung zuständigen Managerin bzw. des für die Einstellung zuständigen Managers.

Nach der Einstellung müssen alle Mitarbeiterinnen und Mitarbeiter die HubSpot-Richtlinie zur akzeptablen Nutzung sowie den Verhaltens- und Ethikkodex (den sogenannten „HubSpot Code of Use Good Judgement“) lesen und anerkennen. Beide Dokumente beschreiben die Verantwortung der Mitarbeiterinnen und Mitarbeiter für den Schutz der Vermögenswerte/Daten des Unternehmens (einschließlich, aber nicht beschränkt auf mobile Geräte und vom Unternehmen bereitgestelltes Equipment).

Richtlinienverwaltung

Damit alle unsere Mitarbeiterinnen und Mitarbeiter dieselben Datenschutzrichtlinien befolgen, dokumentiert und pflegt HubSpot schriftliche Richtlinien und Verfahrensweisen. HubSpot unterhält eine umfassende schriftliche Informationssicherheitsrichtlinie, die neben

vielen anderen Themen die Anforderungen für die Datenverarbeitung, Datenschutzüberlegungen und Reaktionen auf Verstöße enthält.

Die Richtlinien werden mindestens einmal jährlich überprüft und genehmigt sowie in unserem internen Wiki gespeichert. Richtlinien, die von den Mitarbeitenden akzeptiert werden müssen, sind Teil der verpflichtenden jährlichen Schulung.

Sicherheitsschulungen und Sensibilisierung

Mitarbeiterinnen und Mitarbeiter sind maßgeblich am Datenschutz beteiligt, weshalb wir sicherstellen, dass alle HubSpot-Mitarbeitenden ihren Aufgaben gewachsen sind. Allen neuen HubSpot-Mitarbeiterinnen und Mitarbeitern wird bei ihrer Einstellung eine Schulung zum Sicherheitsbewusstsein angeboten, bei der bewährte Sicherheitsverfahren behandelt werden. Neben Bewusstseinsschulungen informiert HubSpot seine Mitarbeiterinnen und Mitarbeiter mit internen Informationsschreiben über aktuelle Entwicklungen oder Initiativen in der Sicherheitsbranche.

Nach der ersten Schulung stehen je nach Position der Mitarbeiterin oder des Mitarbeiters bzw. dem sich daraus ergebenden Datenzugriff weitere spezialisierte Inhalte zur Verfügung. HubSpot bietet zum Beispiel ein Security-Advocates-Programm an, das es Entwicklerinnen und Entwicklern der Produktteams ermöglicht, weitere Schulungen zu Sicherheitsentwicklungen, allgemeinen Risiken, Bedrohungen und Problemen zu absolvieren.

Risikomanagement

HubSpot bietet ein Enterprise-Risk-Management-Programm (ERM) an, das eine dokumentierte ERM-Richtlinie, fortlaufende Risikobewertungen und ein formelles Risikoregister umfasst. Die Aktivitäten zur Risikominderung und -behebung werden über ein Ticketingsystem verfolgt und in festgelegten Intervallen überprüft.

Weitere Einzelheiten zur Risikobewertung und zum Risikomanagementprogramm finden Sie im SOC 2-Bericht (herunterladbar auf hubspot.de/security).

Anbietermanagement

Wir setzen eine Reihe von Drittanbietern ein, die die HubSpot-Produkte ergänzen, um Ihre Anforderungen in den Bereichen Marketing, Vertrieb, Services, Content Management und

Operations zu erfüllen. Wir betreiben ein Programm zum Anbietermanagement, um angemessene Kontrollmechanismen für die Sicherheit und den Datenschutz zu gewährleisten. Das Programm umfasst die Inventarisierung, das Tracking und die Überprüfung der Sicherheitsprogramme der Anbieterinnen und 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 den Anbietenden gesteuert. Unsere Sicherheits-, Rechts- und Compliance-Teams stimmen sich im Rahmen der Überprüfung des Lieferantenmanagements mit unseren Interessensvertretern ab.

Eine Liste unserer Unterauftragsverarbeiter finden Sie auch in unserer Vereinbarung zur Datenverarbeitung.

Physische Unternehmenssicherheit

Die Niederlassungen von HubSpot sind mehrfach gesichert. An allen HubSpot-Niederlassungen weltweit gewährleisten Sicherheitskräfte ein risikofreies Umfeld für HubSpot-Angestellte. Der Zugang wird mittels RFID-Token kontrolliert, die mit den Mitarbeitenden 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.

Schutz von Unternehmensnetzwerken

Zentral verwaltete Anwendungs-Firewalls werden für die Hochverfügbarkeit in den HubSpot-Zweigstellen eingesetzt. Unsere Gastnetzwerke sind von unserem Unternehmensnetzwerk getrennt und werden durch eigene Firewalls geschützt. Die Firewalls filtern nicht autorisierten, eingehenden Datenverkehr aus dem Internet und sind so konfiguriert, dass sie eingehende Netzwerkverbindungen verweigern, die nicht ausdrücklich durch eine Regel genehmigt sind.

HubSpot führt Systemkonformitätsprüfungen durch, bevor die Verbindung eines Geräts mit dem Unternehmensnetzwerk genehmigt wird. Nicht autorisierte Geräte werden sofort getrennt oder in Containment-VLANs verschoben.

Endpunktschutz und Schutz vor Viren/Malware

HubSpot nutzt Endpunktdetektion und -reaktion (EDR) zum Schutz seiner Systeme. So werden wir über von der Norm abweichendes Systemverhalten informiert und können dieses schnell untersuchen und angemessene Maßnahmen ergreifen – entweder durch automatische Ereignis-Trigger oder durch die manuelle Eingrenzung eines Systems. Unsere EDR-Plattform wurde in andere Tools unseres Sicherheitssystems integriert, wodurch ein optimiertes, vielseitiges Ökosystem entsteht, mit dem wir unser Unternehmen effektiv verteidigen können.

Vorfallmanagement

Reaktion auf Vorfälle

Das Team des Security Operations Center (SOC) von 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 zügiges, zuverlässiges Eingreifen. Vordefinierte Vorfalltypen 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 Datenschutzvorfällen 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 bieten je nach Bedarf regelmäßige Updates, um eine angemessene Lösung des Vorfalls zu gewährleisten.

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

Neben unserem SOC verfügt HubSpot auch über ein internes Threat-Hunter-Team, das systematisch Schwachstellen aufdeckt und sicherstellt, dass bewährte Praktiken zur Sicherung unserer Produkte befolgt werden.

Compliance

Sarbanes-Oxley (SOX)

Als börsennotiertes Unternehmen werden die wichtigsten IT-Kontrollen von HubSpot regelmäßig im Rahmen der SOX-Compliance geprüft.

Öffentliche Informationen über die SOX-Compliance von HubSpot und unsere Jahresabschlüsse sind Teil unserer SEC-Dokumente. Weitere Informationen finden Sie auf unserer Investor-Relations-Seite: https://ir.hubspot.com (auf Englisch).

System- und Organisationskontrollen (SOC 2)

HubSpot unterzieht sich jährlich strengen SOC 2 Typ II- und SOC 3-Prüfungen, aus denen hervorgeht, welche Kontrollmaßnahmen wir zur Einhaltung der vom American Institute of Certified Public Accountants (AICPA, Dachverband der US-amerikanischen Wirtschaftsprüfer) festgelegten Trust Service Principles (TSPs) hinsichtlich der Sicherheit, Verfügbarkeit und Vertraulichkeit unserer Kundendaten implementieren. Wir sind stolz auf den hohen Standard unserer Kontrollmechanismen und legen Ihnen nahe, sich an Ihre HubSpot-Ansprechperson zu wenden, um ein Exemplar unseres SOC 2 Typ II-Berichts zu erhalten. Unser SOC 3 steht auf der HubSpot-Seite zum Thema Sicherheit (hubspot.de/security) zum öffentlichen Download bereit.

Verarbeitung und Speicherung von sensiblen Daten

Weitere Informationen über verbotene Datentypen finden Sie in unseren Nutzungsbedingungen (https://legal.hubspot.com/de/terms-of-service). Die HubSpot-Produkte sollten nicht zur Erfassung sensibler Daten wie Kredit- oder Bankkartennummern, Informationen zu privaten Bankkonten, Sozialversicherungsnummern, Reisepassnummern, Führerscheinnummern oder ähnlichen Daten, Finanzauskünften oder Daten zur Beschäftigung oder Gesundheit eingesetzt werden.

Viele Kundinnen und Kunden aus dem Gesundheitswesen nutzen HubSpot in ihrem Frontoffice, ohne sensible Gesundheitsdaten zu verarbeiten. HubSpot ist allerdings keine Lösung zur Verarbeitung oder Speicherung von elektronischen, geschützten Gesundheitsdaten (ePHI), da es weder HIPAA-konform noch HITRUST-zertifiziert ist.

Wenn HubSpot-Kundinnen und -Kunden per Kreditkarte bezahlen, speichert, verarbeitet oder sammelt HubSpot keine Kreditkartendaten, die uns von Kundinnen und Kunden übermittelt werden, und ist nicht PCI-DSS-konform. Wir arbeiten mit vertrauenswürdigen, PCI-konformen Zahlungsverarbeitern zusammen, damit unsere Zahlungstransaktionen sicher abgewickelt werden.

Datenschutz

Der Schutz der Daten unserer Kundinnen und 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 Kundinnen und Kunden im Vordergrund. Unser Datenschutzprogramm umfasst Best Practices, die Anforderungen unserer Kundinnen und Kunden und die ihrer Kontakte sowie regulatorische Vorschriften.

Datenaufbewahrung/-löschung

Ihre Kundendaten werden im HubSpot-System gespeichert, solange Sie aktive Kundin bzw. aktiver Kunde bei uns sind. Die HubSpot-Plattform bietet aktiven Kundinnen und Kunden die Möglichkeit, ihre Daten zu löschen (siehe „Löschung oder Rückgabe personenbezogener Daten“ in unserer Vereinbarung zur Datenverarbeitung von HubSpot) oder ihre Daten zu exportieren (siehe den Artikel in der Wissensdatenbank über den Export Ihrer Inhalte und Daten).

Daten ehemaliger Kundinnen und Kunden werden auf schriftliche Anforderung der Person oder nach Ablauf einer vorgegebenen Frist nach Beendigung sämtlicher Verträge mit der Kundin bzw. dem Kunden entfernt. Daten von Freemium-Kundinnen und -Kunden werden

gelöscht, wenn das Portal nicht mehr aktiv genutzt wird. Daten ehemaliger zahlender Kundinnen und 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.

HubSpot bietet seinen Kundinnen und Kunden derzeit nicht die Möglichkeit, eigene Richtlinien zur Datenaufbewahrung zu definieren.

Verwaltung des Datenschutzprogramms

Die Rechts-, Sicherheits- und diverse andere Teams von HubSpot arbeiten gemeinsam daran, die Effektivität und lückenlose Umsetzung unseres Datenschutzprogramms zu gewährleisten. Informationen über den Schutz Ihrer Daten finden Sie in unserer:

- Datenschutzrichtlinie
- Produkt-Datenschutzrichtlinie
- Vereinbarung zur Datenverarbeitung

Reaktion auf Vorfälle

Unsere Richtlinien, Verfahren und Verpflichtungen zur Meldung von Vertragsverletzungen finden Sie in unserem SOC-Bericht unter dem Abschnitt „Reaktion auf Vorfälle“.

Unsere Verpflichtungen bei Verstößen gegen den Schutz von personenbezogenen Daten finden Sie auch in unserer Datenschutzvereinbarung.

Datenschutz-Grundverordnung (DSGVO)

Die HubSpot-Plattform verfügt über Funktionen, die es unseren Kundinnen und Kunden ermöglichen, ihre Compliance-Anforderungen laut DSGVO zu erfüllen, einschließlich der Möglichkeit, eine DSGVO-Löschung nach einer Bitte um Offenlegung der gespeicherten Daten durchzuführen (siehe diesen Artikel in der Wissensdatenbank). Bitte besuchen Sie unsere DSGVO-Seite unter diesem Link.

Umfang und Verwendung dieses Dokuments

HubSpot setzt bei der Bereitstellung der Lösungen für unsere Kundinnen und Kunden 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.