ZUSAMMENFASSUNG DER SICHERHEITSMASSNAHMEN VON HP

Der Schutz von Kundendaten ist für die Geschäfte von HP von entscheidender Bedeutung. HP nutzt eine Reihe robuster Informationssicherheitskontrollen, einschließlich Richtlinien, Praktiken, Verfahren und Organisationsstrukturen, um die Vertraulichkeit, Integrität und Verfügbarkeit seiner eigenen Informationen und der seiner Kunden (einschließlich personenbezogener Daten gemäß der Definition in den Kunden- und Datenverarbeitungszusätzen von HP) zu gewährleisten. Im Folgenden sind die technischen und organisatorischen Sicherheitsmaßnahmen von HP aufgeführt, die im gesamten Unternehmen angewendet werden.

1. Sicherheitsrichtlinien

HP unterhält weltweit geltende Richtlinien, Standards und Verfahren, die dem Schutz der Daten von HP und seiner Kunden dienen. Die Einzelheiten der Sicherheitsrichtlinien von HP sind vertraulich, um die Integrität der Daten und Systeme von HP zu schützen. Im Folgenden finden Sie aber zusammenfassende Beschreibungen unserer wichtigsten Richtlinien.

2. Abteilung für Informationssicherheit

HP hat eine eigene Abteilung für Informationssicherheit, die für die Leitung und Verwaltung der Informationssicherheitsstrategie und -kontrollen des Unternehmens verantwortlich ist. Ein Informationssicherheits-Framework/-Managementsystem wurde eingerichtet, um die Einhaltung der Sicherheitsrichtlinien und -kontrollen von HP zu gewährleisten und zu bestätigen, dass die Sicherheitsanforderungen der Kunden eingehalten werden. Dieses Framework ist in Anlehnung an das NIST Cybersecurity Framework unterteilt und wird jährlich überprüft.

3. Ressourcenverwaltung

HP verfügt über einen Prozess zur Identifizierung technischer Informationsressourcen, über den alle Ressourcen im Verantwortungsbereich von HP identifiziert und die kritischen Ressourcen kategorisiert werden. Darüber hinaus verfügt HP über eine Reihe von Handhabungsverfahren für die verschiedenen Informationsklassen, einschließlich solcher, die personenbezogene Daten enthalten. Die Handhabungsverfahren betreffen die Speicherung, Übertragung, Kommunikation, den Zugriff, die Protokollierung, Aufbewahrung, Vernichtung, Entsorgung, Vorfallmanagement sowie die Benachrichtigung bei Sicherheitsverletzungen.

4. Zugriffssteuerung

HP nutzt das Prinzip der geringsten Berechtigung für eine logische Zugriffskontrolle. Der Benutzerzugang erfolgt über eine eindeutige Benutzer-ID und ein Kennwort. Die Kennwortrichtlinie von HP umfasst dabei verschiedene Kontrollen in Bezug auf Komplexität, Stärke, Gültigkeit und Kennwortverlauf. Die Zugangsrechte werden regelmäßig überprüft und bei Beendigung des Nutzungszweckes widerrufen.

Es werden Verfahren zur Erstellung und Löschung von Benutzerkonten eingeführt, die im gegenseitigen Einvernehmen vereinbart wurden, um den Zugang zu den Kundensystemen, die während des Auftrags genutzt werden, zu gewähren und zu entziehen.

5. Personalschulung

HP Mitarbeiter müssen die Schulung „Integrität bei HP“ absolvieren, um sicherzustellen, dass sie mit dem Programm, den Richtlinien und Ressourcen vertraut sind, die die Erwartungen von HP in Bezug auf ethisches Verhalten, herausragende Leistungen und Compliance regeln. Die Schulung „Integrität bei HP“ umfasst auch Module zu Sicherheit und Datenschutz, und Mitarbeiter müssen jährlich eine Auffrischungsschulung absolvieren. HP Mitarbeiter müssen außerdem eine jährlich aktualisierte Schulung zum Sicherheitsbewusstsein absolvieren, die sich auf die wichtigsten Sicherheitsrichtlinien konzentriert und die Verantwortlichkeiten der Mitarbeiter in Bezug auf Vorfallmanagement, Datenschutz und Informationssicherheit hervorhebt.

6. Drittparteien und Unterauftragnehmer

HP verfügt über Verfahren zur Auswahl von Unterauftragnehmern, die in der Lage sind, die umfassenden vertraglichen Sicherheitsanforderungen zu erfüllen.

Für Auftragnehmer, die HP eigene oder von HP gehaltene kundeneigene Daten verarbeiten/speichern/übertragen oder Zugang zum HP Netzwerk haben, führt HP Cybersecurity eine Risikobewertung durch, um sicherzustellen, dass diese über ein geeignetes Informationssicherheitsprogramm verfügen. Damit ein solches Programm angemessen ist, muss es physische, technische und verwaltungstechnische Sicherheitsvorkehrungen umfassen. Diese Bewertung muss vorgenommen werden, bevor der Auftragnehmer Zugang zu HP Informationen erhält.

7. Systemsicherheit

Die Entwicklung von Systemen und unterstützender Software innerhalb von HP erfolgt gemäß den Richtlinien nach einer sicheren Entwicklungsmethodik, um die Sicherheit während des gesamten Lebenszyklus von Systemen und Software zu gewährleisten. Der Softwareentwicklungslebenszyklus umfasst alle Anforderungen, von der Initiierung, der Entwicklung/dem Erwerb, der Implementierung, dem Betrieb bis hin zur Außerbetriebnahme und Entsorgung. Alle Systemkomponenten, einschließlich Modulen, Bibliotheken, Diensten und einzelnen Komponenten, werden geprüft, um ihre Auswirkungen auf den Sicherheitsstatus des Gesamtsystems zu bestimmen.

HP hat verschiedene Kontrollen für den Schutz von Anwendungstransaktionen festgelegt. Diese umfassen die Validierung und Überprüfung von Benutzeranmeldedaten, die Vorgabe digitaler Signaturen und Verschlüsselung, die Implementierung sicherer Kommunikationsprotokolle und die Speicherung von Online-Transaktionsdaten auf Servern innerhalb der entsprechenden Netzwerksicherheitszone.

Zudem werden regelmäßig interne Schwachstellen-Scans durchgeführt.

8. Physische und umgebungsbezogene Sicherheit

Alle Einrichtungen von HP sind durch verschiedene physische und elektronische Zugangskontrollen und Überwachungseinrichtungen gesichert. Je nach Art der Einrichtung kann dies Sicherheitspersonal, elektronische Zugangskontrolle und Videoüberwachung (CCTV) umfassen.

Alle HP Mitarbeiter sind registriert und müssen entsprechende Ausweise tragen.

Alle Einrichtungen verfügen über die erforderliche Infrastruktur mit Temperaturregelung und Notstromversorgung, die bei Bedarf mittels USV und/oder Dieselgeneratoren für kritische Dienste bereitgestellt werden kann.

9. Betriebsmanagement

HP hat eine Reihe von Mindestanforderungen für die Absicherung der technologischen Infrastruktur definiert, darunter Workstations, Server und Netzwerkgeräte. Workstation- und Server-Images enthalten vorgehärtete Betriebssysteme. Die Anforderungen variieren dabei je nach Art des Betriebssystems und der implementierten Kontrollen.

HP hat Network Intrusion Detection/Prevention-Systeme (NIDS/NIPS) im Netzwerk implementiert, die rund um die Uhr überwacht und verwaltet werden.

Die HP Sicherheitsrichtlinien und -standards schreiben eine sichere Entsorgung von Speichermedien vor.

10. Kryptografie

HP hat eine Reihe robuster Prozesse für die Kryptografie definiert, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationsressourcen zu gewährleisten. Zugelassene Protokolle verlangen die Verschlüsselung bestimmter Ressourcen, einschließlich solcher, die personenbezogene Daten enthalten.

11. Management von Informationssicherheitsvorfällen

HP folgt einem eigens entwickelten Prozess für das Management von Cybervorfällen, welcher den Zweck, Umfang, Rollen, Zuständigkeiten, Einbindung des Managements, organisatorische Koordination, Implementierungsverfahren sowie die Überprüfung der Einhaltung von Vorschriften umfasst. Dieser Prozess wird jährlich von HP überprüft und aktualisiert.

Zur Durchführung von regelmäßigen Tabletop-Überprüfungen der Prozesse sowie zur Überprüfung von Sicherheitsvorfällen oder -ereignissen wird ein Cyber Incident Response Team zusammengestellt, das sich aus Mitarbeitern von HP Cybersecurity zusammensetzt, die bezüglich der Reaktion auf Vorfälle und Krisenmanagement geschult sind.

12. Geschäftskontinuitätsmanagement

HP unterhält ein globales Programm zur Gewährleistung der Geschäftskontinuität. Dieses Programm verfolgt einen ganzheitlichen, unternehmensweiten Ansatz für eine durchgängige Kontinuität durch eine Reihe von kooperativen, standardisierten und intern dokumentierten Planungsprozessen.

HP überprüft regelmäßig seine Pläne zur Gewährleistung der Geschäftskontinuität, um deren Wirksamkeit sicherzustellen. HP testet und aktualisiert derzeit alle Pläne mindestens einmal im Jahr und stellt sicher, dass alle Personen, die für die Umsetzung dieser Pläne zuständig sind, geschult werden.

Datum der Überarbeitung	Kurzbeschreibung der Änderung	Verantwortliche Person
Mai 2018	Erstveröffentlichung	Raella Dyke
Februar 2022	Aktualisierung	Grettel Acuña