ZUSAMMENFASSUNG DER HP SICHERHEITSMASSNAHMEN

Zum Schutz der Kundendaten hält HP eine Reihe von Informationssicherheitskontrollen ein. Dazu gehören Richtlinien, Praktiken, Verfahren und Organisationsstrukturen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der eigenen und der Kundendaten (einschließlich personenbezogener Daten, wie in HP's Addendum zur Verarbeitung von Kundendaten definiert). Nachstehend geben wir Ihnen ein Überblick über die von HP unternehmensweit eingesetzten technischen und organisatorischen Sicherheitsmaßnahmen.

1. Sicherheitsrichtlinie

HP unterhält global gültige Richtlinien, Standards und Verfahren zum Schutz von HP- und Kundendaten. Die Details der HP-Sicherheitsrichtlinie sind vertraulich, um die Integrität der Daten und IT-Systeme zu schützen. Im Folgenden finden Sie jedoch Zusammenfassungen unserer wichtigsten Richtlinien.

2. Organisation für Informationssicherheit

HP verfügt über eine Organisation für Informationssicherheit, die für die Steuerung und Verwaltung der verabschiedeten Informationssicherheitsstrategie und -kontrollen verantwortlich zeichnet. HP unterhält ein Informationssicherheits-Managementsystem zur Einhaltung der HP-Sicherheitsrichtlinien und -kontrollen sowie der Sicherheitsanforderungen der Kunden. Dieses Managementsystem orientiert sich am NIST Cybersecurity Framework und wird jährlich überprüft.

3. Management von IT-Systemen und Endgeräten

HP verfügt über einen Prozess zur Identifizierung eingesetzter technischer IT-Systeme und Endgeräte (Server, PCs, Smartphones etc.). Mit Hilfe dieses Prozesses identifiziert HP alle in seiner Verantwortung befindlichen IT-Systeme und Endgeräte und kategorisiert diese nach Kritikalität. Darüber hinaus setzt HP dokumentierte Verfahren zur Handhabung der einzelnen Gerätekategorien ein, einschließlich derer, die personenbezogene Daten enthalten. Diese Verfahren betreffen Speicherung, Übertragung, Kommunikation, Zugriff, Protokollierung, Aufbewahrung, Vernichtung, Entsorgung, Störungsmanagement und Meldung von Verstößen.

4. Zugriffskontrolle

Der Benutzerzugriff erfolgt über eine eindeutige Benutzerkennung und ein Kennwort. Die HP Kennwortrichtlinie hat komplexe Steuerelemente für Komplexität, Stärke, Gültigkeit und Kennwortverlauf definiert. Zugriffsrechte werden regelmäßig überprüft und bei Ausscheiden eines Mitarbeiters widerrufen.

Es wurden Verfahren zur Erstellung und Löschung von Benutzerkonten implementiert, um den Zugriff auf die für die Datenspeicherung eingesetzten IT-Systeme zu gewähren und zu widerrufen.

5. Personal-Training

HP-Mitarbeiter müssen das Training „Integrity at HP“ absolvieren, so dass sichergestellt ist, dass neue Mitarbeiter mit dem Programm, den Richtlinien und Ressourcen vertraut sind, die die Vorgaben von HP hinsichtlich ethischem Verhalten, Verantwortung und Konformität regeln. “Integrity at HP“ beinhaltet u.a. Module für Sicherheit und Datenschutz. Außerdem müssen die Mitarbeiter einen jährlichen „Auffrischungskurs“ absolvieren. HP-Mitarbeiter durchlaufen außerdem ein regelmäßiges Training zum Thema Sicherheitsbewusstsein, das sich auf grundlegende Sicherheitsrichtlinien konzentriert und die Verantwortung der Benutzer in Bezug auf Störungsmanagement, Datenschutz und Informationssicherheit betont.

6. Dritte und Subunternehmer

HP verfügt über die erforderlichen Prozesse zur Auswahl von solchen Subunternehmern, die in der Lage sind, umfassende vertraglich geschuldete Sicherheitsanforderungen zu erfüllen.

7. Systemsicherheit

Gemäß den HP-Richtlinien folgt die Entwicklung von Systemen und unterstützender Software innerhalb von HP einer sicheren Routine, um die Sicherheit von Daten während des gesamten System- / Software-Lebenszyklus zu gewährleisten. Der Software-Entwicklungs-Lebenszyklus definiert die Anforderungen für Initiierung, Entwicklung bzw. Erwerb, Implementierung, Betrieb und Entsorgung. Alle Systemkomponenten, zu denen Module, Bibliotheken, Dienste und diskrete Komponenten gehören, werden ausgewertet, um deren Auswirkung auf den Sicherheitszustand des Gesamtsystems zu ermitteln.

HP hat Kontrollen zum Schutz von Applikationstransaktionen definiert. Zu diesen Kontrollen gehören: Validieren und Verifizieren von Benutzeranmeldedaten, Vorschreiben von digitalen Signaturen und Verschlüsselung, Implementieren sicherer Kommunikationsprotokolle, Speichern von Online-Transaktionsdetails auf Servern in der entsprechenden Netzwerksicherheitszone.

Interne Schwachstellen-Scans werden vierteljährlich sowie nach signifikanten Änderungen durchgeführt.

8. Physische und Umweltsicherheit

HP-Standorte werden durch unterschiedliche Kombinationen von physischen und elektronischen Zugriffskontrollen und Überwachungsfunktionen gesichert. Je nach Standort kann es sich dabei um Sicherheitsbedienstete, elektronische Zugriffskontrollen und/oder Videoüberwachung handeln.

Alle HP-Mitarbeiter sind registriert und sind verpflichtet, Firmenausweise tragen.

Die Standorte verfügen, soweit erforderlich, über die notwendige Infrastruktur-Unterstützung mit Temperaturregelung und Stromunterbrechung unter Einsatz von UPS und / oder Dieselgeneratoren zur Unterstützung kritischer Dienste.

9. Betriebsmanagement

HP hat für die Technologie-Infrastruktur von Workstations, Servern und Netzwerkgeräten Mindestanforderungen festgelegt. Workstation und Server Images enthalten Betriebssysteme mit festen Voreinstellungen zur Erhöhung der Systemsicherheit. Die Anforderungen an die Voreinstellungen hängen vom Typ des Betriebssystems und den implementierten geltenden Kontrollen ab.

HP setzt in seinen Netzwerken Angriffserkennungs- und Präventionssysteme (NIDS / NIPS) ein, welche rund um die Uhr überwacht und verwaltet werden.

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

10. Kryptographie

HP hat diverse Prozesse für die Kryptographie definiert, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationsressourcen sicherzustellen. Genehmigte Protokolle erfordern die Verschlüsselung bestimmter Anwendungen, einschließlich derer, die personenbezogene Daten enthalten.

11. Informationssicherheit Störungsmanagement

HP verfolgt einen entwickelten Cyber-Störungsmanagementprozess, der auf Zweck, Umfang, Rollen, Verantwortlichkeiten, Management-Eskalation, organisatorische Koordination, Implementierungs-verfahren und Konformitätsüberprüfung abzielt. HP überprüft und aktualisiert diesen Prozess jährlich.

Ein Cyber-Störungsreaktionsteam, zu dem auch HP Cybersecurity-Mitarbeiter gehören, die in der Reaktion auf Störungen und Krisenmanagement geschult sind, wird zur regelmäßigen Überprüfung des Prozesses und aller Störungen oder Ereignisse zusammengestellt.

12. Geschäftskontinuitätsmanagement

HP unterhält ein global ausgerichtetes Programm zur Aufrechterhaltung des Geschäftsbetriebes. Dieses Programm verfolgt einen ganzheitlichen, unternehmensweiten Ansatz zur Sicherstellung einer durchgängigen Business Kontinuität mittels Umsetzung diverser kollaborativer, standardisierter und intern dokumentierter Planungsprozesse.

HP setzt die definierten Pläne zur Business Kontinuität regelmäßig um und stellt damit die Wirksamkeit der Pläne sicher. Alle Pläne werden mindestens einmal jährlich getestet. Weiterhin findet eine regelmäßige Schulung der involvierten Mitarbeiter statt.