Dell APEX-Informationssicherheitsmaßnahmen – Nachtrag

Die Dell APEX-Services beruhen auf einem Modell der geteilten Sicherheitsverantwortung, bei dem Sie und Dell jeweils bestimmte Zuständigkeiten haben, da Dell APEX-Services in Ihren Räumlichkeiten oder an einem Colocation-Standort gehostet werden und im Allgemeinen kein Hosting von Kundeninhalten auf Servern in von Dell verwalteten Rechenzentren beinhalten. Ihre Zuständigkeiten sind in der jeweiligen Angebotsbeschreibung festgelegt.

Dell hat die folgenden Unternehmenssicherheitsmaßnahmen für die Dell APEX-Services eingerichtet und sich zu ihrer Aufrechterhaltung verpflichtet. Dells Verantwortung hinsichtlich der Sicherheit der Dell APEX-Services ist auf diese Maßnahmen in Verbindung mit den in der jeweiligen Angebotsbeschreibung genannten Sicherheitsmaßnahmen beschränkt. Wenn in diesem Dokument nichts anderes festgelegt ist, kommt allen großgeschriebenen Begriffen in diesem Dokument die ihnen in den Dell APEX Bedingungen zugewiesene Bedeutung zu.

Funktion	Maßnahmen
Informationssicherheitsprogramm	Dell hat ein Informationssicherheitsprogramm eingeführt und wird es aufrechterhalten (einschließlich der Verabschiedung interner Richtlinien und Standards), das folgende Ziele verfolgt: (a) Ermittlung der nach vernünftigem Ermessen vorhersehbaren Sicherheitsrisiken für die gegebenenfalls vorhandenen Teile der Rechenzentren, Server, Netzwerkausrüstungen, Firewalls und Hostsoftwaresysteme von Dell, die für die Bereitstellung der Dell APEX-Services verwendet werden („**Dell Netzwerk**“, und (b) Einsatz wirtschaftlich vertretbarer Anstrengungen zur Minderung identifizierter Sicherheitsrisiken für das Dell Netzwerk, soweit und wie Dell dies für angemessen hält, einschließlich regelmäßiger Risikobewertungen und Tests. Dell hat einen oder mehrere Sicherheitsbeauftragte ernannt, die für die Koordination, das Monitoring und die Durchsetzung des Informationssicherheitsprogramms verantwortlich sind. Dell unterhält ein Programm für das Bedrohungs- und Sicherheitslückenmanagement, das die fortlaufende Überwachung des Dell Netzwerks auf Sicherheitslücken beinhaltet. Die Identifizierung von Sicherheitslücken erfolgt unter Einsatz einer Vielzahl von Quellen/Methoden, darunter Anbieter, Sicherheitsforscher, Scans auf Sicherheitslücken, Red-Team-Tätigkeiten, Penetrationstests und Reporting durch Mitarbeiter. Veröffentlichte Sicherheitslücken von Drittanbietern werden darauf geprüft, ob sie auf die Umgebung von Dell zutreffen. Scans und Bewertungen von Sicherheitslücken erfolgen routine- und regelmäßig in der Anwendungsinfrastruktur von Dell. Diese Prozesse sollen dazu dienen, eine proaktive Identifizierung und Korrektur von Sicherheitslücken zu ermöglichen sowie die Compliance-Anforderungen von Dell sowie regulatorische Auflagen zu unterstützen.

Sicherer Entwicklungslebenszyklus und Reaktion auf Sicherheitslücken	Dell unterhält ein Programm für einen sicheren Entwicklungslebenszyklus zur Festlegung der Schritte, die ergriffen werden müssen, um sicherzustellen, dass seine Angebote in angemessenem Umfang und entsprechend der Struktur eines förmlichen Governance-Programms mit einem definierten sicheren Entwicklungslebenszyklus bewertet, entwickelt und verpackt wurden. Im Zusammenspiel mit dem Informationssicherheitsprogramm von Dell unterstützt dieses Programm den Umgang mit dem Thema Sicherheit über den gesamten Entwicklungs- und Wartungslebenszyklus des Dell APEX-Systems hinweg. Dell wendet einen strikten Prozess zur fortwährenden Beurteilung und Verbesserung seiner Praktiken der sicheren Entwicklung und Reaktion auf Sicherheitslücken an und vergleicht diese regelmäßig mit den Standardpraktiken der Branche. Nach der Untersuchung und Validierung einer gemeldeten Sicherheitslücke im Dell APEX-System wird Dell versuchen, eine geeignete Abhilfemaßnahme in Übereinstimmung mit der von Dell veröffentlichten Richtlinie zur Behebung von Sicherheitslücken, die derzeit unter https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy zu finden ist, zu identifizieren, zu entwickeln und zu qualifizieren. Dell informiert seine Kunden gegebenenfalls durch Sicherheitshinweise über Abhilfemaßnahmen. Dell ist bestrebt, Abhilfemaßnahmen wo zutreffend innerhalb eines wirtschaftlich angemessenen Zeitraums zur Verfügung zu stellen. Die Reaktionszeiten hängen von vielen Faktoren ab, wie z. B. dem Schweregrad, der Komplexität der Abhilfemaßnahmen oder der betroffenen Komponente.
Asset Management	Dell überwacht und verwaltet die physischen und logischen Ressourcen des Dell Netzwerks. Zu den Ressourcen, die Dell verfolgen kann, und zu den Kontrollen, die Dell durchführen kann, gehören beispielsweise: (a) Softwareressourcen wie Anwendungen und Systemsoftware, (b) physische Ressourcen wie Server, Desktop-PCs/Laptops, Backup-/Archivierungsbänder, Drucker und Kommunikationsgeräte und (c) Informationsressourcen wie Datenbanken, Disaster-Recovery-Pläne, Business-Continuity-Pläne, Datenklassifizierung und archivierte Daten. Dell klassifiziert Ressourcen auf der Basis ihrer Bedeutung für den Geschäftsbetrieb bzw. ihrer Vertraulichkeitsstufe. Aufgrund dieser Klassifizierung kann der Zugang zu der betreffenden Ressource nach Bedarf beschränkt werden.

Personalsicherheit	Im Rahmen des Einstellungsprozesses müssen die Mitarbeiter von Dell eine Geheimhaltungsvereinbarung unterzeichnen und durchlaufen einen Überprüfungsprozess gemäß und im Einklang mit dem geltenden Recht. Obwohl Dell sich das Recht zur Überprüfung seiner Richtlinien und der Umsetzung der Personalsicherheit nach eigenem Ermessen vorbehält, führt Dell den aktuellen Richtlinien entsprechend und gemäß lokalem Recht und je nach lokaler Verfügbarkeit bei der Einstellung die folgenden Überprüfungen durch: Drogen-Screening, Abfrage von Sozialversicherungsangaben, Prüfung Vorstrafenregister, Überprüfung der Angaben zu Bildungsweg und Beschäftigung sowie Überprüfung der Eignung für die Beschäftigung. Dell versucht, den aktuellen Branchenstandards für vergleichbare Unternehmen in der Branche, in der Dell tätig ist, zu entsprechen. Jedoch kann Dell seine Personalsicherheitsmaßnahmen oder Überprüfungsprozesse nicht an die besonderen Erwartungen eines bestimmten Kunden anpassen. Drittanbieter oder externe Contractors werden entweder von Dell überprüft, als Bedingung des Vertrags überprüft oder nach einem von Dell genehmigten Prüfprozess vom Contractor als überprüft bestätigt. Dell wendet ein Disziplinarverfahren an, wenn Mitarbeiter sich nicht an die Informationssicherheitspraktiken von Dell halten. Dies betrifft u. a. die Praktiken, die zur Erfüllung seiner Verpflichtungen und Anforderungen in den Bereichen Sicherheit, Verfügbarkeit und Vertraulichkeit eingeführt wurden. Dell veranstaltet eine jährliche Schulung des Sicherheitsbewusstseins für das gesamte entsprechende Personal von Dell und verpflichtet die entsprechenden Unterauftragnehmer, eine solche Schulung für ihr Personal zu veranstalten.
Physische Sicherheit	Dell hält Richtlinien und Kontrollen aufrecht, die den physischen Zugang zu Einrichtungen, in denen sich physische Komponenten des Dell Netzwerks befinden, auf entsprechend befugtes Personal beschränken und die einen unbefugten Zutritt zu diesen Einrichtungen verhindern sollen. In Einrichtungen, die physische Komponenten des Dell Netzwerks beherbergen (z. B. Rechenzentren), werden risikobasierte Kontrollen durchgeführt. Zu diesen Zugriffskontrollen gehören ggf. Wachpersonal, Sicherheitsprotokolle, Monitoring, Alarme, eingeschränkter Zugang zu gesicherten Bereichen, Schutz von Zugangswegen, Videoüberwachung, Schlüsselkarten und/oder Zwei-Faktor-Authentifizierung. Diese Bestimmung gilt für von Dell verwaltete Colocation-Standorte.
Netzwerksicherheit	Das Dell Netzwerk ist für Dell elektronisch zugänglich, soweit dies für die Bereitstellung der Dell APEX-Services erforderlich ist. Dell hält Richtlinien und Zugriffskontrollen aufrecht, mit denen der zulässige Zugriff auf das Dell Netzwerk von jedem

	Verbindungspunkt aus verwaltet werden kann. Dies umfasst die Nutzung von Firewalls und Authentifizierungskontrollen. Durch die risikobasierte Implementierung bestimmter Kontrollen schützt sich Dell vor der böswilligen Nutzung von Ressourcen und dem Einsatz von Schadsoftware im Dell Netzwerk. Zu diesen Kontrollen können u. a. gehören: Sicherheitsrichtlinien; restriktive Zugriffskontrollen; separate Entwicklungs- und Testumgebungen; Erkennung von Malware auf Servern, Desktop-PCs und Laptops; Scannen von E‑Mail-Anhängen auf Malware; Scans zur Überprüfung der Systemkonformität; Intrusion-Prevention-Monitoring und Reaktion auf Angriffe; Protokollierung und Alarmierung bei wichtigen verdächtigen Ereignissen; Verfahren zur Informationsverarbeitung nach Datentyp, E‑Commerce-Anwendung und Netzwerksicherheit; Nutzung externer Ressourcen sowie Scannen auf Sicherheitslücken in Systemen und Anwendungen. Dell verlangt die Verschlüsselung von Daten bei Übertragung und im gespeicherten Zustand, sofern dies erforderlich und mit seinem Informationssicherheitsprogramm vereinbar ist. Dell verwendet beim Remote-Zugriff auf Kundensysteme auf offenen Netzwerken Verschlüsselungstechniken und geeignete Protokolle (z. B. TLS). Dell speichert seine Verschlüsselungsschlüssel, wenn diese nicht verwendet werden, in genehmigten Lösungen, die für in der Branche anerkannte Key-Management-Praktiken entwickelt wurden.
Zugriffskontrollen	Dell richtet geeignete Zugriffskontrollen ein, die dem Schutz vor unbefugtem Zugriff auf das Dell Netzwerk dienen. Zur Verringerung des vorsätzlichen oder anderweitigen Missbrauchsrisikos wird der Zugriff gemäß den Prinzipien des „geringsten Privilegs“ und des „Kennenmüssens“ kontrolliert. Zu den von Dell genutzten Zugriffskontrollen gehören Zugriffsüberprüfung, Wartung von Servicekonten und privilegierter Zugriff auf die Anwendungen, Systemlevel-Einstellungen für den Zugriff und die Erstellung von Berichten im Zusammenhang mit dem Zugriff. Dell wendet dem Branchenstandard entsprechende Praktiken an, darunter ggf. die Zwei-Faktor-Authentifizierung, um Nutzer des Dell Netzwerks zu identifizieren und zu authentifizieren. Dell erfordert die Verwendung sicherer Kennwörter im gesamten Dell Netzwerk. Dell (a) untersagt es Nutzern des Dell Netzwerks, Kennwörter in unverschlüsselter Form auf jeglichen Systemen weiterzugeben, niederzuschreiben, per E-Mail oder Instant Messaging zu versenden oder sie zu speichern, und (b) sperrt Konten, wenn mehrmals nacheinander ein falsches Kennwort eingegeben wurde. Dell verwendet branchenübliche Verfahren zur Verbesserung der Zugriffskontrollen, darunter: (a) automatische Beendigung von Nutzersitzungen, wenn diese nicht genutzt werden, (b) Erfordernis der Identifizierung und des Kennworts für die Wiedereröffnung,

	(c) Schutz vor externem Zugriff durch anerkannte branchenübliche Firewalls, deren Verbindung zum Internet gegebenenfalls durch eine VPN-Verbindung gesichert ist; (d) Masking von Kennwörtern, wenn diese angezeigt oder eingegeben werden, und (e) eine angemessene und dem Branchenstandard entsprechende Kennwortverschlüsselung bei der Übermittlung.
Incident-Management	Dell verwendet ein Incident-Response-Framework, um sich auf Sicherheitsvorfälle vorbereiten, darauf reagieren, sie kontrollieren und ihre Auswirkungen minimieren zu können. Das Framework umfasst Verfahren, die im Falle eines Sicherheits-Incidents zu befolgen sind, darunter: (a) ein internes Incident Response-Team mit einem Reaktionsverantwortlichen; (b) ein Untersuchungsteam, das eine Ursachenanalyse durchführt und die betroffenen Parteien ermittelt; (c) interne Reporting- und Benachrichtigungsverfahren; (d) die Dokumentation von Abhilfemaßnahmen und Korrekturplänen; und (e) eine Überprüfung der Ereignisse nach dem Incident.
Business-Continuity-Management	Dell unterhält Business-Continuity-Pläne („**BCP(s)**“) für die Wiederherstellung nach einer Geschäftsunterbrechung und die Wiederaufnahme des normalen Geschäftsbetriebs, sobald dies vernünftigerweise möglich ist. Dell unternimmt unter den gegebenen Umständen angemessene und zeitnahe Versuche, Sie im Falle einer Störung des Geschäftsablaufs mit wesentlichen Auswirkungen auf Ihre(n) Dell APEX-Service(s) zu kontaktieren.