Trusted Data Center und Storage-Infrastruktur

DELL Technologies

intel.

Storage-Infrastruktur des Trusted Data Centers

Mittelständische Unternehmen stehen bei der Storage-Infrastruktur für ihre Rechenzentren oft vor denselben Herausforderungen wie ihre Enterprise-Pendants. Beiden fehlt es jedoch an denselben Ressourcen, um diese zu bewältigen. Kapazitäten, Ausfallzeiten, Datendiebstahl und die Nichteinhaltung behördlicher Auflagen wirken sich negativ auf diese Unternehmen aus, während sie gleichzeitig danach streben in einer zunehmend wettbewerbsorientierten Umgebung kontinuierliche Innovationen vorantreiben. Es muss sichergestellt werden, dass wertvolle Daten und IT-Ressourcen jederzeit verfügbar, langlebig, skalierbar und geschützt sind. Wie können mittelständische Unternehmen angesichts dieser herausfordernden Marktdynamik erfolgreich sein?

Die erfolgreichsten Unternehmen verpflichten sich der Priorisierung eines sicheren Rechenzentrums, einschließlich der Storage-Infrastruktur. In Abbildung 1 ist die Beziehung zwischen Trusted Data Center-Technologien, verbesserten betrieblichen Ergebnissen und letztlich geschäftlichen Erfolgen dargestellt.

Beziehung zwischen Best Practices und Technologien für ein Trusted Data Center und Geschäftsergebnisse.

Sicherheit im Rechenzentrum und bewährte Best Practices können in Bezug auf Folgendes gemessen werden:

- Häufigere Infrastruktur-aktualisierungen
- Engagement des Unternehmens für eine sichere Infrastrukturtechnologie
- Erfolg bei der Implementierung sicherer Infrastruktur-technologien

Sicherheit im Rechenzentrum und bewährte Best Practices führen zu besseren Technologieergebnissen wie z. B:

- Weniger Ausfälle
- Schnellere Service- und Datenwieder-herstellungen
- Weniger Datenverlust, Sicherheitsvorfälle
- Bessere Möglichkeit zur Erfüllung von Compliancevorgaben

Schließlich ermöglicht eine bessere Technologie- und Sicherheitsperformance einen größeren geschäftlichen Erfolg, darunter:

- Schnellere Markteinführung
- Höhere Kundenzufriedenheit
- Größerer Marktanteil
- Schnellere Umsatzsteigerung

Quelle: Enterprise Strategy Group

Die drei Säulen für den Betrieb eines Trusted Data Center sind:

1. Die Rechenzentrums-infrastruktur regelmäßig aktualisieren und außer Betrieb nehmen

2. Bewährte Technologien bereitstellen

3. Diese Technologien implementieren

Trusted Data Center Storage-Technologien umfassen moderne Datensicherheitsfunktionen wie Verschlüsselung, integrierte Firmware-Sicherheitsfunktionen sowie Methoden zur Data Protection wie Backupfrequenz und Replikation.

Minimierung der Risiken, die Ihre Daten gefährden

Mittelständische Unternehmen müssen die Verbesserung der Sicherheit und Zuverlässigkeit ihrer IT-Umgebungen, einschließlich der Storage-Infrastruktur, priorisieren. Die Minimierung negativer geschäftlicher Auswirkungen durch Storage-Unterbrechungen wie Sicherheitsverletzungen oder Datenverlust, verbessert die Wettbewerbsfähigkeit und den Erfolg mittelständischer Unternehmen in ihren Märkten.

Storage-Services sind für den Geschäftsbetrieb unerlässlich, denn jede Unterbrechung dieser Services kann negative Auswirkungen haben.

- **Cybersicherheitsrisiken können einem Unternehmen im Vergleich zu Mitbewerbern schaden**
- **Ausfälle können den Customer Service unterbrechen**
- **Datenverluste beeinträchtigen die Produktivität und Verstöße gegen Compliance-Vorschriften haben oft direkte finanzielle Folgen**

Als Teil der Sicherheitsstrategie sollten Aktualisierungen und Außerbetriebnahmen der Infrastrukturen eingeplant werden. Eine neuere Infrastruktur umfasst im Allgemeinen eine Reihe von Sicherheits- und Data-Protection-Funktionen, die bei älteren Lösungen möglicherweise fehlen. Kurz gesagt: Unternehmen, die mehr in Infrastrukturaktualisierungen investieren, sind in einer besseren Position, verbesserte Ergebnisse zu erzielen.

Unternehmen, die mehr in Infrastrukturaktualisierungen investieren, **können bessere Ergebnisse erzielen.**

Neben der Aktualisierung der Infrastruktur verpflichten sich erfolgreiche Unternehmen außerdem zu zusätzlichen Best Practices für die Storage-Infrastruktur, unter anderem:

- **Verschlüsselung sensibler Daten, um diese vor Diebstahl oder Beschädigung zu schützen**
- **Investitionen in Infrastrukturlösungen mit marktführenden Sicherheitsfunktionen, die in ihre Firmware integriert sind**
- **Replikation sensibler Daten auf sekundäre Storage-Systeme, um die Verfügbarkeit und Wiederherstellbarkeit zu maximieren**

Erfolgreiche Unternehmen arbeiten in zuverlässigeren, belastbareren und schwer zu kompromittierenden Umgebungen. Als Gruppe erleben sie messbar weniger Sicherheitsvorfälle, die zu Datenverlust oder -beschädigung führen, weniger Situationen der Nichtcompliance mit internen Governance- oder gesetzlichen Vorschriften und weniger Ausfälle, nach denen zudem die Wiederherstellung schneller durchgeführt wird. Eine hohe Technologieperformance trägt wiederum dazu bei, schneller als Mitbewerber auf dem Markt zu sein, die Kundenzufriedenheit zu verbessern und sowohl den Marktanteil als auch den Umsatz zu steigern.

Ein weiterer Punkt in Sachen IT- und Geschäftsrisiken ist das Engagement bei erfolgreichen unternehmen für Compliance. Complianceanforderungen, sowohl interne als auch behördliche, können streng sein. Für mittelständische Unternehmen mit begrenzten Ressourcen ist eine effiziente Methode zur Sicherstellung der Compliance von entscheidender Bedeutung. Gleichzeitig muss die angewandte Methodik effektiv sein, da viele mittelständische Unternehmen die Bußgelder für Nichtcompliance der behördlichen Auflagen schwer treffen würden.

Verfügbarkeit der Storage-Infrastruktur sicherstellen

Es gibt zahlreiche Ursachen für Ausfälle bei der Storage-Verfügbarkeit. Eine Naturkatastrophe kann einen Standort zum Erliegen bringen, menschliche Fehler können zu einem Serviceausfall führen oder ein System – ob Server-, Storage- oder Netzwerkkomponente – kann einfach ausfallen. IT-Unternehmen, die eine neuere Infrastruktur betreiben und mehr in Technologielösungen mit hoher Sicherheit und hoher Zuverlässigkeit investieren, erzielen erstklassige Ergebnisse.

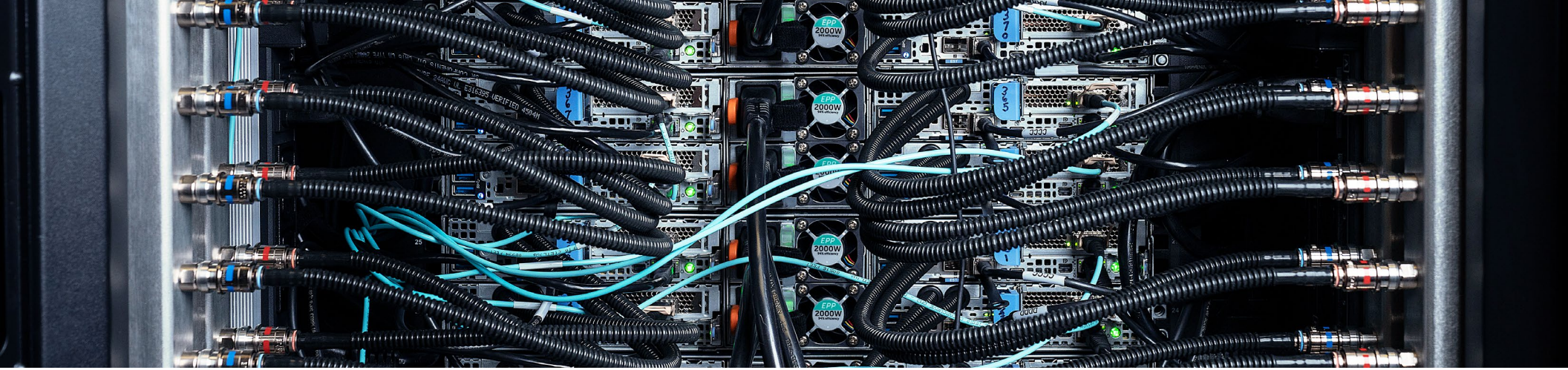
Die Verfügbarkeit der Storage-Infrastruktur ist sowohl für den laufenden Betrieb als auch für die kontinuierliche Entwicklung und Bereitstellung neuer Geschäftsservices unerlässlich. Ein Storage-Ausfall hat unmittelbare und offensichtliche Auswirkungen auf Kunden und andere, die auf diese Services angewiesen sind. Weniger offensichtlich sind die Auswirkungen auf die Entwicklungsteams. Softwareentwicklungspraktiken haben sich größtenteils von monolithischen Wasserfallmethoden zu flexiblen, kontinuierlichen Entwicklungs- und Bereitstellungsmodellen entwickelt. Der Verlust von Storage-Services kann die Entwicklungsbemühungen stoppen, die Entwicklungsarbeit kosten und erhebliche Recovery-Zeit einfordern.

Unternehmen müssen
die Daten ihrer Kunden ständig sichern.

Verbesserung der geschäftlichen Agilität mit einem Trusted Data Center Storage

Unternehmen, die sich auf Trusted Data Center-Technologie, einschließlich Storage-Services, konzentrieren, haben bessere Möglichkeiten für Innovationen, die Bereitstellung neuer Produkte und die Erfüllung von Kundenerwartungen. Und diese Erwartungen werden immer deutlicher, da Verbraucher und andere Unternehmen von den ständig verfügbaren digitalen Services profitieren. Diese steigende Nachfrage nach kontinuierlichem Zugriff auf Geschäftsservices erhöht den Druck, sowohl hochverfügbare als auch hochgradig skalierbare Anwendungen bereitzustellen. Unternehmen, die diese Art von Anwendungen betreiben können, sind wettbewerbsfähiger und in der Lage zu wachsen.

Hohe Verfügbarkeit und Skalierbarkeit allein reichen nicht aus, um die Anforderungen heutiger digitaler Services zu erfüllen. Unternehmen müssen die Daten ihrer Kunden ständig sichern. Datenschutzverletzungen sind zu häufig und selbst wenn Verbraucher möglicherweise mit einigen Sicherheitslecks rechnen, verursachen diese Angriffe finanzielle Kosten und Reputationskosten. Mittelständische Unternehmen können eine Trusted Data Center Storage-Infrastruktur nutzen, um das Risiko von Datenschutzverletzungen, Ransomware und anderen disruptiven Cybersicherheitsbedrohungen zu minimieren.



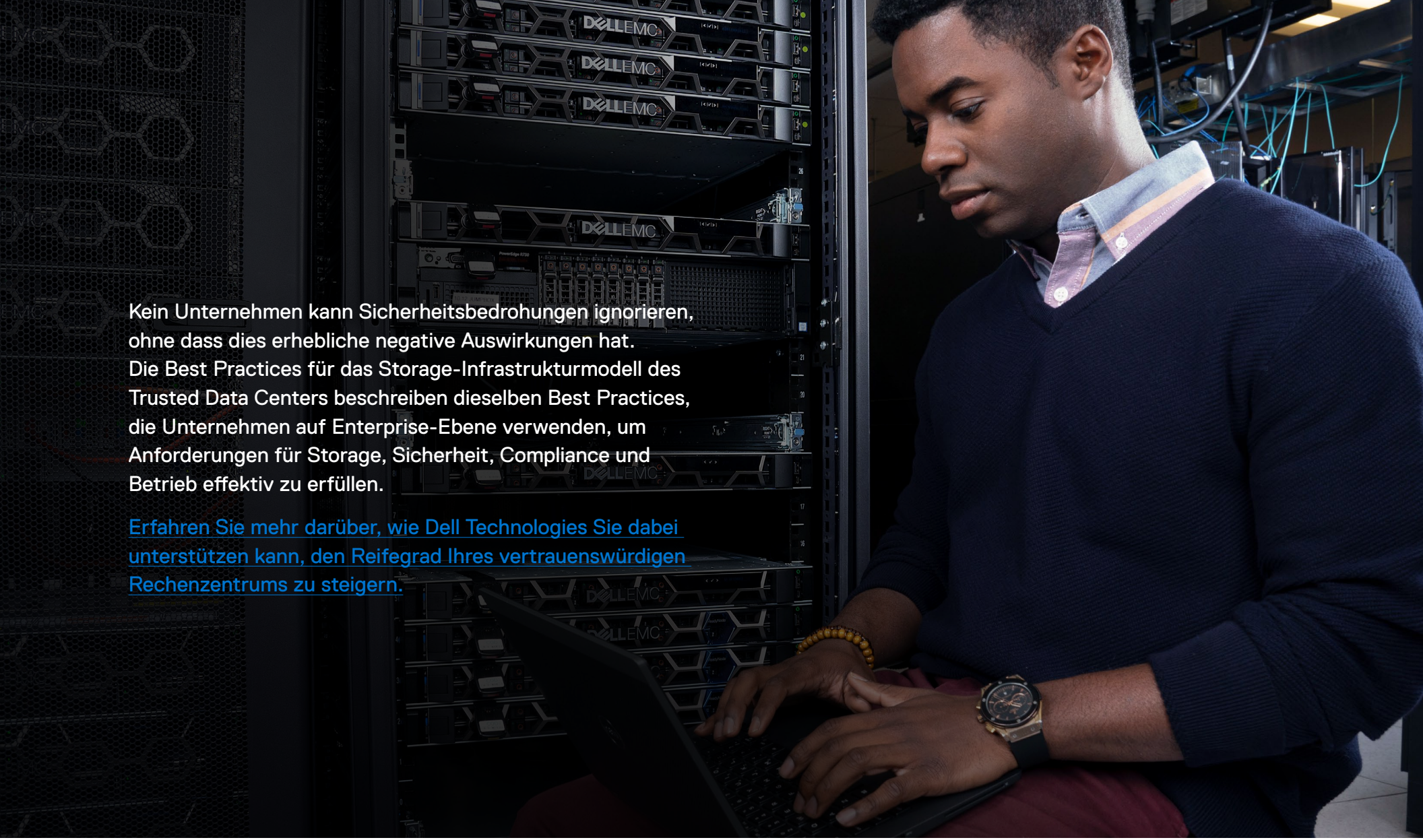
Unternehmen sollten darauf hinarbeiten, die Einhaltung der hier beschriebenen Best Practices zu gewährleisten. Dazu zählt:

Führen Sie häufiger Aktualisierungen der Server- und Storage-Infrastruktur durch und verwenden Sie Lösungen mit anspruchsvolleren Sicherheits- und Data Protection-Funktionen.

Priorisieren Sie Serverlösungen mit ausgereiften „integrierten“ Sicherheitsfunktionen. Neuere Server sind zwar in der Regel sicherer als ältere Server, dennoch gibt es bestimmte Sicherheitsfunktionen, auf die Sie sich konzentrieren sollten:

- Die Möglichkeit, alle Systemupdates auf kryptografische Authentifikation zu prüfen
- Die Automatische Sperrung von Konfigurationseinstellungen
- Die Möglichkeit, das System vollständig zu löschen

Stellen Sie die Implementierung dieser Best Practices sicher, indem die finanziellen und personellen Ressourcen bereitgestellt werden, die für eine effektive Implementierung der Best Practices erforderlich sind.



Kein Unternehmen kann Sicherheitsbedrohungen ignorieren, ohne dass dies erhebliche negative Auswirkungen hat. Die Best Practices für das Storage-Infrastrukturmodell des Trusted Data Centers beschreiben dieselben Best Practices, die Unternehmen auf Enterprise-Ebene verwenden, um Anforderungen für Storage, Sicherheit, Compliance und Betrieb effektiv zu erfüllen.

Erfahren Sie mehr darüber, wie Dell Technologies Sie dabei unterstützen kann, den Reifegrad Ihres vertrauenswürdigen Rechenzentrums zu steigern.

DELL Technologies

intel.