Schutz von Daten an entfernten Standorten und in Homeoffices

Drei Tipps für mehr Sicherheit in Außenstellen von Organisationen von Florian Malecki, International Product Marketing Senior Director bei StorageCraft

Veränderungen in einem gewissen Maß sind normal – aber in der letzten Zeit war das Tempo der Veränderungen alles andere als normal. Für IT-Fachleute, die ihre Unternehmen oder Kunden bei der Umstellung auf ein weitreichendes Arbeiten in Homeoffices unterstützt haben, war das Tempo der Veränderungen sogar geradezu schwindelerregend.

IT-Manager müssen sich vielen Herausforderungen stellen, darunter einem explosionsartigen Datenwachstum oder der zunehmenden Bedrohung durch Ransomware-Attacken. Zusätzlich haben die Verwaltung und das Management von Backup und Wiederherstellung sowohl für Zweigstellen als auch für Homeoffices den Druck erhöht. Diese außerplanmäßige Herausforderung ist für viele IT-Manager in der heutigen, zunehmend verteilten IT-Umgebung, schlicht zu viel.

Grundsätzlich stellt Datenzugang von Filialen oder Homeoffices für Unternehmensdaten ein größeres Risiko als Zugang vom Firmensitz dar. Die Sicherheit in Remote-Netzwerken ist in der Regel weitaus schwächer als die Sicherheit in internen Netzwerken. Darüber hinaus lassen extern arbeitende Mitarbeiter ihre Arbeitsstationen oft unbeaufsichtigt und sichern ihre Daten nicht regelmäßig. Das macht Organisationen zusätzlich anfällig für Cyberattacken.

Sicherheit, Backup und Wiederherstellung für verteilte Standorte und Homeoffices stellen eine große Herausforderung dar. Natürlich war dies schon lange vor der COVID-19-Pandemie der Fall. Beim Schutz und der Wiederherstellung von Daten haben sich Unternehmen schon immer mehr auf das Rechenzentrum und weniger auf die Außenstellen konzentriert. Da Unternehmen mit verteilten Standorten mit knappen IT-Budgets zu kämpfen haben, wurde der Firmenzentrale Priorität eingeräumt, sodass Remote-Offices und Zweigstellen nur wenige oder gar keine dedizierten IT-Ressourcen zur Verfügung hatten.

Dieses Problem hat sich durch COVID-19 und die explosionsartige Zunahme von Heimarbeit verschärft. Daten sind nun weitläufiger verteilt, was die Anfälligkeit noch weiter erhöht. Um die Daten an entfernten Standorten effektiv zu verwalten und zu schützen, ist mehr Support erforderlich. Aber diesen gibt es meist nicht. Die einfachsten Schritte, wie beispielsweise das Sichern von Daten, finden in einer entfernten Umgebung und ohne zentrale IT-Unterstützung oft nicht statt.

Dabei gibt es Lösungen, die helfen können, diese Herausforderungen elegant zu meistern. Mit nur drei Tipps können Unternehmen ihre Daten an entfernten Standorten und in Homeoffices besser verwalten und schützen – ohne dass die Kosten explodieren oder die vorhandenen Ressourcen über Gebühr strapaziert werden.

1: Testen der Wiederherstellung von Daten

Ein kontinuierliches und sicheres Backup ist unerlässlich. Aber ebenso wichtig ist die vollständige und schnelle Wiederherstellung verlorener Daten.

Sicherheit geben Tests, und man sollte die Backups regelmäßig dahingehend prüfen, ob sich die Daten zuverlässig wiederherstellen lassen.

Zusätzlich gilt es, die Datensicherheit zu testen, um in der IT-Infrastruktur und bei den Mitarbeitern Lücken in der Abwehr ausfindig zu machen. Gleichzeitig sollten Remote-Mitarbeiter regelmäßig geschult werden, damit sie die neuesten Cyberattacken erkennen können. Hacker lernen ständig dazu, und nur mit Schulungen können Mitarbeiter die neuesten Bedrohungen identifizieren und mit ihnen Schritt halten.

2: Den Umgang mit Daten und Cyberhygiene fördern

Indem heute viele Mitarbeiter in entfernten Standorten arbeiten, ist es für Unternehmen schwierig, Daten zu speichern und Backups in Filialnetzwerken zu verwalten. Unternehmen sollten regelmäßig mit den Mitarbeitern kommunizieren und sie daran erinnern, ihre Daten konsistent und an mehreren Orten zu sichern. Datensicherungen sollten keinesfalls nur auf einem USB-Flash-Laufwerk gespeichert sein, sondern an mehreren Speicherorten, etwa auf einer Festplatte oder in der Cloud. Sollten Daten hauptsächlich in der Cloud gespeichert sein, ist eine Offline-Kopie sehr sinnvoll.

Darüber hinaus ist eine gute Cyberhygiene wichtig. Insbesondere diejenigen Mitarbeiter, die an entfernten Standorten arbeiten, sollten regelmäßig daran erinnert werden, die Software auf ihren Geräten zu aktualisieren und alle verfügbaren Sicherheitsmaßnahmen, einschließlich Firewalls und Anti-Malware-Tools, einzuschalten. Das Versäumnis, Software zu aktualisieren und Sicherheitspatches zu installieren, ist ein häufig auftretendes Problem, das einer raschen Verbreitung von Ransomware Tür und Tor öffnet. Diese

Nachlässigkeit führt zu Datenverlusten und kostet Unternehmen jedes Jahr Milliarden an Euro. Das Schließen dieser Sicherheitslöcher reduziert die Gefahr einer Kompromittierung von Daten erheblich.

3: Cloudbasierte Sicherung und Wiederherstellung

Die Datensicherung und -wiederherstellung für entfernte Standorte sollte ebenso leicht zu verwalten sein wie in der Unternehmenszentrale. Die gute Nachricht ist, dass es einfach zu implementierende, kostengünstige, cloudbasierte Lösungen gibt, welche die Daten an entfernten Standorten effektiv sichern und schützen – ohne dass dedizierte Ressourcen an IT-Spezialisten oder Budgets zur Verfügung gestellt werden müssen.

Einige der Lösungen machen es Unternehmen und den IT-Teams sehr leicht, durch eine Plug-and-play-Integration die automatische Provisionierung des Speichers und cloudbasierter Plattformen einfach zu verwalten. Alles, was dazu nötig ist, ist das Einschalten des Geräts und eine Verbindung mit dem Internet. So funktioniert zuverlässiger Datenschutz innerhalb von wenigen Minuten.

Seit dem Ausbruch von COVID-19 haben Unternehmen und Systemhäuser hervorragende Arbeit geleistet, indem sie vielen Mitarbeitern das Arbeiten von zu Hause ermöglicht haben. Jetzt ist es an der Zeit, dafür zu sorgen, dass die Daten auch sicher und geschützt aufbewahrt werden. Glücklicherweise lässt sich Data Protection mit den richtigen Tools und der richtigen Herangehensweise effizient realisieren.

###

Folgen Sie StorageCraft auf Twitter, LinkedIn und Facebook.
Lesen Sie die neuesten Artikel zum Thema Datensicherung und Datenwiederherstellung im StorageCraft Blog.

Unternehmenskontakt
Jock Breitwieser
StorageCraft Technology Corp.
+1 408.800.5625
jock.breitwieser@storagecraft.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
storagecraft@tc-communications.de
www.tc-communications.de