arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

**Reales Risiko für Daten, wenn Mitarbeiter „außerhalb" arbeiten.**

*Von Sven Richter, Marketing Manager DACH bei Arcserve*

Die COVID-Pandemie löste eine schnelle und weit verbreitete Verlagerung hin zur Remote-Arbeit aus. Dieser Trend hält aus gutem Grund bis heute an, denn er hat viele Vorteile. Beispielsweise bietet Remote-Arbeit Mitarbeitern mehr Flexibilität bei der persönlichen Zeitplanung, erspart das Pendeln zur Arbeitsstelle, fördert das Wohlbefinden und steigert oftmals die Produktivität. Allerdings gibt es wie bei allen Trends nicht nur Vorteile, sondern auch Schattenseiten. Zum Beispiel hat die Zunahme der Remote-Arbeit zu Bedenken hinsichtlich der Cybersicherheit geführt, da Mitarbeiter, die außerhalb des Büros arbeiten, vielfach nicht über die entsprechenden Sicherheitsfunktionen verfügen.

Die Frage ist, ob und wie Unternehmen darauf reagieren? Laut einer neuen Studie von Arcserve verfügen beispielsweise nur 38 Prozent der Finanzdienstleister über eine Sicherungs- und Wiederherstellungslösung für externe Mitarbeiter. Das ist riskant, denn Unternehmen, die nicht über eine Sicherheitslösung für externe Mitarbeiter verfügen, setzen sich einer Vielzahl ernsthafter Bedrohungen aus – darunter Datenverlust, Nichteinhaltung gesetzlicher Vorschriften und Betriebsunterbrechungen.

Bei Finanzdienstleistern ist die Situation jedoch weniger dramatisch, da sich in dieser Branche ein Großteil der Daten nicht auf den Geräten der Mitarbeiter befindet. Strenge Kontrollen und Überwachungsfunktionen sorgen dafür, dass so wenig Daten wie möglich auf den einzelnen Geräten liegen. Mitarbeiter müssen via Remote Virtual Desktops anmelden oder Daten auf SharePoint oder OneDrive speichern, die beide cloudbasiert sind.

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

**Wo Remote-Backup zu kurz greift**

Der Finanzsektor mag in Bezug auf die Datensicherheit vergleichsweise gut aufgestellt sein, doch in anderen Branchen ist die Lage prekärer. Betrachtet man die Remote-Arbeit in Bereichen, wo die Vorschriften und Sicherheitsmaßnahmen in der Regel weniger streng sind, lassen sich ernsthafte Probleme feststellen. In vielen Industriezweigen ist es Einzelpersonen gestattet, Daten auf ihren Geräten zu speichern, was ein Problem darstellt. Dabei ist insbesondere die Datensicherung von Remote-Geräten eine Herausforderung, weil die Unternehmen in vielen Fällen die Geräte nicht selbst verwalten. Stattdessen konzentrieren sie sich lediglich auf die Kontrolle des Zugriffs auf unternehmens- oder webbasierte Ressourcen wie Microsoft 365, NetSuite und Salesforce.

Tatsache ist, dass die meisten Unternehmen Remote-Geräte nicht angemessen sichern. Selbst wenn sie es versuchen, ist der Schutz dieser Geräte schwierig, da diese sich ständig im mobilen Einsatz befinden. Herkömmliche Sicherungs- und Wiederherstellungsmethoden greifen oft zu kurz, wenn der Laptop nicht verfügbar oder offline ist. Längst nicht alle Sicherungs- und Wiederherstellungslösungen setzen die Sicherung automatisch fort, wenn das Gerät wieder online ist. Dieses Problem kann zu einem Datenverlust über Tage hinweg führen.
Daher sollte es angesichts der zunehmenden Remote-Arbeit das Ziel sein, so viele Daten wie möglich in der Cloud oder auf Unternehmensservern zu speichern und die Abhängigkeit von einzelnen Geräten zu verringern. Bei einem Angriff oder wenn ein Laptop verloren geht, beziehungsweise beschädigt wird, bleiben die Daten auf diese Weise erhalten und zugänglich.

**Vier Grundpfeiler für den Schutz von Remote-Daten**

Im Zusammenhang mit der Remote-Arbeit und der Datensicherheit gibt es vier wichtige und bewährte Verfahren:

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

1. Daten zentralisieren
   Auch wenn Personen Kopien von Daten auf Remote-Arbeitsplätzen haben, sollte das Ziel darin bestehen, die Daten auf Unternehmensservern oder cloudbasierten Lösungen wie Office 365, Salesforce, NetSuite oder einer ähnlichen Plattform zu zentralisieren.

2. Sichere Remote-Geräte
   Ob Laptop, Tablet oder Heimcomputer – alle Geräte sind ein Tor zu den Unternehmenssystemen. Der Laptop beispielsweise ist das Portal, über das Mitarbeiter auf Anwendungen wie Salesforce und Office 365 zugreifen. Das Ziel ist es, die Sicherheit dieser Geräte zu verbessern, damit dieses Tor nicht von böswilligen Akteuren genutzt wird. Der Ansatz sollte eine robuste Endpunktsicherheit, starke Authentifizierung und regelmäßige Updates umfassen, um die Geräte vor Malware, unbefugtem Zugriff und bekannten Sicherheitslücken zu schützen.

3. Anwender schulen und trainieren
   Viele Angriffe oder Datenverluste sind erst aufgrund von kompromittierten Benutzeranmeldedaten möglich. Die wenigsten dieser Attacken konzentrieren sich lediglich auf Anmeldeinformationen von Super-Administratoren oder hochrangigen Mitarbeitern. Auch normale Benutzeranmeldeinformationen können ausgenutzt werden, um Schaden anzurichten, insbesondere auf Plattformen wie Microsoft 365. Darum ist es entscheidend, dass Anwender gut geschult und wachsam sind. Unternehmen sollten eine Sicherheitskultur anstreben, in der jeder Mitarbeiter seine Rolle bei der Aufrechterhaltung der Cybersicherheit versteht und sich für den Schutz sensibler Daten und Systeme verantwortlich fühlt.

arcserve®
Protect what's priceless.
380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

4. Kontinuierliche Aktualisierung der Richtlinien und Verfahren
   Diese Best Practice gilt für Sicherheits-, Sicherungs-, Wiederherstellungs- und Benutzerzugangsrichtlinien. Diese sollten regelmäßig aktualisiert werden, um mit den Veränderungen in der Infrastruktur Schritt zu halten, etwa mit der Einführung neuer Anwendungen. An den Beispielen der größeren Ransomware-Vorfälle wird deutlich, dass viele davon mit veralteten Anmeldedaten ausgeführt wurden. Wenn beispielsweise Mitarbeiter ein Unternehmen verlassen und ihre Anmeldedaten nicht umgehend widerrufen werden, entsteht eine Schwachstelle. Wenn Unternehmen mit der Aktualisierung von Richtlinien in Verzug geraten, führt dies zu einer Diskrepanz zwischen den Richtlinien und dem Schutz der Daten.

**Fazit**

Die globale Verlagerung hin zur Remote-Arbeit birgt sowohl Chancen als auch Risiken. Sie bietet mehr Flexibilität und Anpassungsfähigkeit, erhöht jedoch auch Gefahren für die Cybersicherheit und steigert das Risiko für Datenverlust. In Anbetracht dieser Herausforderung sollten Unternehmen auf Erfahrungswerte vertrauen und übergeordnete Sicherheitsprinzipien beherzigen. Und da die Remote-Arbeit gekommen ist, um zu bleiben und bereits heute ein integraler Bestandteil jeder modernen Organisation ist, sollte mit allen nötigen Mitteln für die Datensicherheit gesorgt werden.

Folgen Sie Arcserve auf LinkedIn oder X und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

**Über Arcserve**

Arcserve gehört weltweit zu den Top-5-Herstellern von Datensicherungslösungen und bietet als Anbieter von Unified Data Resilience Lösungen eine einheitliche Plattform für die Ausfallsicherheit von Daten an. Das Unternehmen stellt das breiteste Spektrum an Best-in-Class-Lösungen für die Verwaltung, den Schutz und die Wiederherstellung aller Datenumgebungen zur Verfügung. Die Lösungen von Arcserve eignen sich für KMUs und Großunternehmen, unabhängig von deren Standort und der Komplexität der Infrastruktur. Sie beseitigen die Komplexität und bieten gleichzeitig erstklassigen, kosteneffizienten, flexiblen und massiv skalierbaren Datenschutz und Sicherheit für alle Datenumgebungen. Dazu gehören On-Prem-, Off-Prem- (einschließlich DRaaS, BaaS und Cloud-to-Cloud), hyperkonvergente und Edge-Infrastrukturen. Dank der vier Jahrzehnte langen Erfahrung des Unternehmens mit preisgekrönten IP-Lösungen und der kontinuierlichen Konzentration auf Innovation können Partner und Kunden, darunter MSPs, VARs, LARs und Endbenutzer, sicher sein, dass sie den schnellsten Weg zu Daten-Workloads und -Infrastrukturen der nächsten Generation finden. Arcserve ist ein zu 100 Prozent channelorientiertes Unternehmen, das in über 150 Ländern vertreten ist und mit 19.000 Vertriebspartnern die kritischen Datenbestände von 235.000 Kunden schützt. Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf X oder LinkedIn.

**Unternehmenskontakt**
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

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