arcserve®
Protect what's priceless.

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

Die 7 Phasen der Cyberresilienz: Wie KMUs die Achterbahnfahrt für den Datenschutz meistern

Von René Claus, EMEA MSP Sales Director bei Arcserve

Heutzutage sind Daten das mit Abstand wertvollste Gut jedes modernen Unternehmens – unabhängig von der Branche und egal, wie groß es ist. Wenn Unternehmen durch einen technischen Ausfall, einen Cyberangriffs oder eine Naturkatastrophe den Zugriff auf die Daten verlieren, sind Teilbereiche oder sogar der komplette Betrieb gefährdet. Aus diesem Grund sind die Ausfallsicherheit und die Resilienz eine zwingende Notwendigkeit.

Resiliente Unternehmen im Sinne des Datenschutzes und der Datensicherheit verfügen über Prozesse, die ihnen eine schnelle Erholung von jeder datenkritischen Situation garantieren. Allerdings ist längst nicht jedes Unternehmen mit dieser Widerstandsfähigkeit ausgestattet. Im Gegenteil – die meisten KMUs sind es nicht. Eine kürzlich von Arcserve durchgeführte internationale Studie bestätigt, dass nur 23 Prozent der kleinen und mittelständischen Unternehmen über ausgereifte Resilienzstrategien für die Datensicherheit verfügen.

Das ist nicht ideal, gleichwohl aber keine Überraschung. Denn kleine und mittlere Unternehmen konzentrieren sich hauptsächlich auf ihr Kerngeschäft. Sie verwenden nahezu die gesamte Zeit darauf, das Unternehmen zu führen, Marketing und Vertrieb zu managen und ihre Kunden zu bedienen. Die Aufrechterhaltung des Business hat oberste Priorität. Diese Fokussierung schränkt jedoch die Fähigkeit, zusätzliche Aufgaben wie Cybersicherheit zu bewältigen, deutlich ein.

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

Darüber hinaus bestehen nach wie vor weit verbreitete Missverständnisse im Bereich des Cyberschutzes. Zwar kennen KMUs die potenzielle Gefahrenlage durch Cyberbedrohungen, allerdings sind viele der Meinung, dass vornehmlich größere Unternehmen ins Fadenkreuz der Angreifer geraten. In Wahrheit jedoch selektieren Cyberkriminelle nicht nach Branche oder Unternehmensgröße. Sie haben es auf jedes potenzielle Opfer abgesehen, unabhängig davon, wie klein oder groß es sein mag. Ergo sind KMUs keineswegs immun gegen Cyberangriffe - und je früher sie diese Tatsache realisieren, desto höher ist die Chance, rechtzeitig für Schutz und Datensicherheit zu sorgen.

Die 7 Phasen der Cyberresilienz

Beim Menschen und in der Psychologie existiert ein Prozess, den Fachleute mit "sieben Phasen der Trauer" beschreiben. Hierbei geht es um eine psychologische Abfolge, wenn Menschen einen tiefgreifenden Verlust oder Trauerfall erleben - einschließlich Schock, Leugnung, Wut und Depression. Wendet man diese "sieben Trauerphasen" auf KMUs mit Datenschutzproblemen an, stellen sich diese wie folgt dar:

1. **Schock und Leugnung:** Das ist der Zeitpunkt, an dem sich ein mittelständisches Unternehmen erstmals der potenziellen Risiken für seine Daten bewusst wird. Es ist schockiert über das Ausmaß des potenziellen Schadens durch unterschiedliche Bedrohungen. Manche Unternehmen reagieren anfangs mit einer Verleugnung, weil es den Verantwortlichen schwerfällt zu glauben, dass ihr Unternehmen durch eine derartige Bedrohung Schaden nehmen könnte.
2. **Schmerz und Schuldgefühle:** Wenn KMUs beginnen, den Ernst der Lage zu begreifen, verursachen mögliche Verluste oder Schäden am Unternehmen Schmerzen. Es ist zudem möglich, dass sich

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

Schuldgefühle entwickeln, insbesondere wenn das Unternehmen den Datenschutz in der Vergangenheit nicht ernst genommen hat und unnötigen Risiken eingegangen ist.

3. **Wut und Verhandlungsbereitschaft:** Im Unternehmen kann sich wegen der Umstände, die zur Bedrohung der Daten geführt hat, Wut breitmachen. Durch Cyberkriminelle oder Nachlässigkeiten kann es dazu kommen, dass nach einer schnellen Lösung gesucht wird, was langfristig nicht automatisch zu einer wirksamen Strategie führen muss.
4. **Depression:** Die Erkenntnis, dass der Aufwand und die Ressourcen, die für einen wirksamen Schutz von Daten erforderlich sind, kann zu einer Art Depressionen führen. Der Grund: Durch die Komplexität des Datenschutzes und die potenziellen Folgen eines Datenverlusts fühlen sich mittelständische Unternehmen schnell überfordert.
5. **Aufwärtstrend:** Sobald mittelständische Unternehmen beginnen ihre Datensicherheit mit konkreten Schritten zur verbessern, geht es aufwärts. Sie erkennen, dass der Prozess anfangs zwar komplex, jedoch machbar ist. Der erste Schritt besteht zum Beispiel darin, die kritischen Betriebssysteme zu definieren. Es gibt solche, die bei einer Kompromittierung nur eine geringfügige Störung verursachen wogegen andere das gesamte Unternehmen zum Stillstand bringen, oder vielleicht sogar ruinieren. Deshalb sollte ein Unternehmen unbedingt herausfinden, wo kritische Daten gespeichert werden und welche Systeme für das Funktionieren des Unternehmens erforderlich sind.
6. **Wiederaufbau und Aufarbeitung:** In dieser Phase arbeitet das Unternehmen aktiv an seinen Datensicherungsstrategien. Es implementiert neue Maßnahmen, verbessert seine Systeme, schult Mitarbeiter und führt die notwendigen Arbeiten zur Verbesserung der Datenresilienz durch. Das Unternehmen kann beispielsweise seine

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

Sicherungs- und Wiederherstellungsprozesse verbessern, indem es Datenkopien an getrennten Orten speichert, um Datenverluste, beispielsweise bei einem Cyberangriff, zu verringern. Außerdem kann es eine unveränderliche Datenspeicherung implementieren, bei der alle 90 Sekunden ein Snapshot der Daten erstellt wird. Das hilft bei der Datenwiederherstellung, etwa wenn durch Ransomware Daten verschlüsselt werden.

7. **Akzeptanz und Hoffnung:** Mittelständische Unternehmen akzeptieren die enorme Wichtigkeit der Datenausfallsicherheit und den damit verbundenen Aufwand. Sobald die richtigen Kontrollen und Warnsysteme vorhanden sind, ist das Unternehmen in einer viel besseren Ausgangsposition, um unbefugten Zugriff zu verhindern und unerwartete Vorfälle zu beheben. Dann haben die Unternehmen auch wieder Hoffnung, besser vorbereitet auf Datenbedrohungen zu reagieren und sich von möglichen Datenvorfällen schnell zu erholen.

Mehrwerte eines Dienstleisters

Aufgrund mangelnder Ressourcen konzentrieren sich viele mittelständische Unternehmen intensiv auf ihr Tagesgeschäft. Nicht selten kommen dabei die IT und insbesondere der Datenschutz zu kurz. Deshalb ist es für viele KMUs eine sinnvolle Option, mit einem spezialisierten Dienstleister zusammenzuarbeiten, der über ausgewiesene Expertise in den Bereichen Datensicherung, Cybersicherheit und Datensicherheit verfügt. Die Zusammenarbeit mit einem Dienstleister, der sich mit Best Practices auskennt und mit führenden Lösungsanbietern zusammenarbeitet, erweitert nicht nur das IT-Knowhow im Unternehmen, sondern sorgt gleichzeitig für einen soliden Plan für die Datensicherheit und die Einhaltung der Datenschutzvorschriften.

arcserve®
Protect what's priceless.

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

Dabei sind naturgemäß auch die Kosten für KMUs ein wichtiges Thema. Während größere Unternehmen ausreichend Personal oder sogar eine ganze Abteilung für die Cybersicherheit und Datensicherung abstellen können, ist das bei vielen KMUs keine realistische Option. Durch die Zusammenarbeit mit einem Service-Provider kann ein mittelständisches Unternehmen kostengünstig auf die benötigten Verfahren und Fachkenntnisse zugreifen. Dank einer solchen Partnerschaft können sie sich auf ihr Kerngeschäft und das Unternehmenswachstum konzentrieren, während sich sachkundige Experten um die Ausfall- und Wiederherstellungsstrategien kümmern.

Es steht viel auf dem Spiel und die Zuweisung eines Budgets für die Datensicherheit ist von entscheidender Bedeutung. Spezialisierte Service Provider führen skalierbare Lösungen im Portfolio, die den individuellen Bedarf von Unternehmen passgenau und zu einem angemessenen Budget abdecken können. Mithilfe von flexiblen Tools und unterschiedlichen Methoden kann ein solider Backup- und Recovery-Plan aufgestellt werden. Damit ist auch für mittelständische und kleinere Unternehmen gewährleistet, dass sie mit einer überschaubaren Investition optimal auf potenzielle Datenvorfälle vorbereitet sind.

# # #

Folgen Sie Arcserve auf LinkedIn oder Twitter 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 fast drei 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 Twitter 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