Als Unternehmen auf Backups verzichten? Grob fahrlässig!

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	1.0
Versionsdatum:	2022-09-07

Designed by www.slon.pics from Freepik

Vorwort

Daten sind das Gold des 21. Jahrhunderts! Das wird Ihnen nicht nur jeder ITler bestätigen - auch Unternehmen, welche schon einen oder mehrere Datenverluste zu verzeichnen haben, wissen wie kostbar die Datenbestände sind.

Gerade aus diesem Grund sind Ihre Daten immer vielfältigeren Bedrohungen ausgesetzt! Bedrohungen lauern aber nicht nur von externen Angreifern, sondern sind auch des Öfteren den eigenen Mitarbeitern geschuldet. Hier erfahren Sie, welche die gängigsten Gefahren für Ihre Daten sind. Im Anschluss werden Sie erkennen, wie wichtig moderne Backup-Strategien sind.

Bedrohungen

1. Unwissenheit und Ignoranz
Sie werden sich denken: "Dann muss man sich halt informieren." Und genau das ist der entscheidende Punkt! Wenn die Entscheider die Notwendigkeit moderner Backup-Strategien nicht erkennen, nicht erkennen wollen oder das Thema aufgrund vor der Angst hoher Kosten meiden, sind Geschäftsdaten permanent in Gefahr. Jedes Unternehmen wird früher oder später einen

Datenverlust verzeichnen - die Frage ist nur, in welchem Ausmaß.

2. Veraltete Software
Ein fehlendes regelmäßiges Patch-Managment erhöht das Risiko von Datenverlust enorm. Dabei sollte nicht nur das Betriebssystem, sondern auch die auf dem System installierte Software regelmäßig aktualisiert werden. Werden Systeme nicht kontinuierlich mit den neuesten Updates versorgt, steigt damit auch die Gefahr eines Softwarefehlers oder Ausfalls. Zudem ist eine veraltete Software ein gefundenes Fressen für Hackerangriffe.

3. Menschliches Versagen
Ich denke jeder kennt das Szenario: Spät am Nachmittag - die Konzentration schwindet und schwub hat man aus Versehen eine falsche Datei gelöscht. Mit einer durchdachten Backup-Strategie sichern Sie sich gegen solche Vorfälle ab.

4. Vorsätzliche Löschung
Leider muss man sagen, dass dieses Szenario auch durch mutwillige Zerstörung von Daten existiert. Es kommt immer wieder vor, dass sich entlassene Mitarbeiter am Unternehmen rächen wollen und kurzer Hand alle Daten löschen auf die sie Zugriff haben. Nicht nur deshalb sollte man allen Mitarbeitern auch nur Zugriff auf Daten freischalten mit denen sie tatsächlich auch arbeiten müssen.

5. Datendiebstahl
Daten können genau wie physische Gegenstände entwendet werden. Es muss sich hier nicht einmal um einen Hackerangriff oder einen abtrünnigen Mitarbeiter handeln, welcher vertrauliche Informationen zur Konkurenz mitnimmt - auch eine verlorene oder gestohlene externe Festplatte bzw. ein USB-Stick können einen Datenverlust zufolge haben.

6. Ransomware
Ransomware sind Schadprogramme, welche Daten auf einem Computer verschlüsseln. Die Täter erpressen ihre Opfer anschließend mit einer Lösegeldzahlung um die verschlüsselten Daten wieder freizugeben. Diese Form der Cyberkriminalität wächst weiterhin drastisch - Tendenz steigend. Eine globale Studie zeigt, dass alleine in Deutschland knapp 69% der Unternehmen schon von einem Ransomware-Angriff betroffen waren.

7. Hackerangriffe, Trojaner und Viren
Neben der oben genannten Ransomware gibt es natürlich noch zahlreiche andere Trojaner, Würmer oder Viren, die Ihre IT-Infrastruktur zum Erliegen bringen können. Auch hier empfiehlt sich, nicht darauf zu hoffen, dass Sie verschont bleiben.

8. Technisches Versagen
Neben den menschlichen Gefahren, darf man auch technische Fehler nicht außer Acht lassen! Es kann immer wieder vorkommen, dass Festplatten oder gar ihr gesamter Server ausfällt. Mit einer geeigneten Backup-Strategie, mit unterschiedlichen Speicherorten und -medien, verhindern Sie den Verlust Ihrer geschäftskritischen Daten.

9. Fehlerhafte Backup-Strategien
Auch wenn Ihre Daten gesichert werden, garantiert das noch lange nicht die Verfügbarkeit im Ernstfall. Auch ein Backup kann fehlerhaft sein, vorloren gehen oder unvollständig sein. In der Praxis hat sich daher die 3-2-1-Regel durchgesetzt: Erstellen Sie *drei* Kopien auf *zwei* unterschiedlichen Speichermedienarten und lagern Sie mindestens *eines* davon an einem externen Speicherort.

10. Elementargewalten
Viele Unternehmer schenken dieser Gefahr keinerlei Beachtung, da die Wahrscheinlichkeit einer Naturkatastrophe zugegebenermaßen vergleichsweise gering zu den oben genannten Punkten ist. Aber glauben Sie mir: Es kommt vor! Sie dürfen auch nicht außer Acht lassen, dass Ihre Daten und Datensicherungen durch Brände, Überschwemmungen und Sturmschäden zerstört werden könnten. Dies muss auch nicht zwangsläufig in Ihrem Unternehmen geschehen - auch große Rechenzentren können davon betroffen sein (Am Rhein brennt Europas Datenschatz). Umso wichtiger ist es, mehrere verschiedene Backupziele zu nutzen.

Fazit

Seien Sie nicht naiv! Es stellt sich nicht die Frage ob ein Unternehmen von einem Datenverlust betroffen sein wird - die Frage lautet wann und in welchem Ausmaß wird der Datenverlust sein. Schützen Sie sich vor diesen Bedrohungen! Sichern Sie Ihre Server, Workstations und auch Cloud-Daten nach dem Großvater-Vater-Sohn-Prinzip und beachten Sie dabei die 3-2-1-Regel. Sprechen Sie uns an - wir beraten Sie gerne.

Revision #2
Created 7 September 2022 12:24:35 by Christian Sigl
Updated 12 September 2022 10:33:05 by Christian Sigl