Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

Datensicherung

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

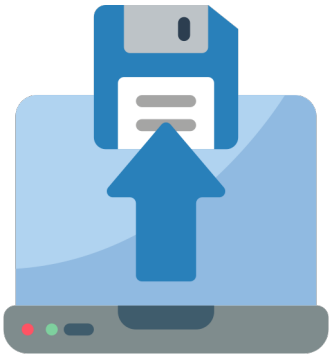
Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Datensicherung – Was ist das?

Datensicherungen, auch **Backup** genannt, sind für Unternehmen und Organisationen von entscheidender Bedeutung, um ihre Cybersicherheit zu stärken. Die zunehmende Digitalisierung und die ständige Bedrohung durch Cyberangriffe machen es unerlässlich, geeignete Maßnahmen zu ergreifen, um sensible **Daten zu schützen** und die **Geschäftskontinuität** sicherzustellen.

Backups bezeichnen **Sicherungen von Daten auf verschiedenen Datenträgern** in den Räumen des Unternehmens und in der Cloud. Eine Datensicherung ist eine Kopie der Unternehmensdaten, die in regelmäßigen Abständen erstellt wird, um im Falle eines Datenverlusts oder einer Beschädigung der Originaldaten eine **Wiederherstellung** zu ermöglichen. Datensicherungen sind ein wichtiger Bestandteil des **Disaster Recovery Plans** von Unternehmen und Organisationen.



Wem nutzen Datensicherungen?

Jedes **Unternehmen**, jede **Institution**, jede **Privatperson** ist heute auf die Verfügbarkeit von Daten angewiesen. Ohne Daten fehlt für die meisten Betriebe die **Geschäftsgrundlage**.

Dementsprechend ernst sollte die Anfertigung eines Backups genommen werden: Jede und jeder sollte regelmäßig die eigenen Daten sichern, um im Fall eines Cybervorfalls geschützt zu sein. Hier gilt: **Kein Backup – kein Mitleid.**

Wie funktioniert eine Datensicherung und welche Varianten gibt es?

Im Allgemeinen besteht der Prozess der Datensicherung aus folgenden Schritten: Zunächst müssen die **Daten identifiziert** werden, die gesichert werden müssen. Dazu gehören in der Regel Datenbanken, Anwendungen, E-Mails und Dokumente. Anschließend muss die geeignete **Datensicherungsmethode** ausgewählt werden. Dies hängt von verschiedenen Eigenschaften ab, wie der Art der Daten, der Häufigkeit der Änderungen und dem verfügbaren Speicherplatz. Standard ist das Prinzip einer täglichen, wöchentlichen und monatlichen Sicherung der Daten. Im Anschluss muss die entsprechende **Software** eingerichtet werden. Dabei müssen Parameter wie der Zeitplan für die Datensicherung, der Speicherort und die Art der Sicherung festgelegt werden. Sobald die Datensicherung konfiguriert ist, kann die eigentliche **Datensicherung** durchgeführt werden. Je nach Variante kann dies **automatisch oder manuell** erfolgen. Danach ist es wichtig, die Integrität der gesicherten Daten zu **überprüfen**. Hierfür können verschiedene Methoden wie ein Datenabgleich mit dem Original oder die Durchführung von Testwiederherstellungen eingesetzt werden. Manche Datensicherungsprogramme bieten interne Prüfroutinen zur Prüfung der Integrität des Backups.

Je nach den Bedürfnissen des Betroffenen kommen verschiedene weitreichende Methoden infrage. Bei einer **vollständigen Datensicherung** werden alle Daten auf einem Datenträger gespeichert. Eine vollständige Datensicherung kann zeitaufwändig sein und erfordert eine große Menge an Speicherplatz. Eine **inkrementelle Datensicherung** speichert nur die Änderungen an den Daten seit der letzten Datensicherung. Dadurch wird Speicherplatz gespart und die Sicherungsdauer reduziert. Eine **differentielle Datensicherung** speichert alle Änderungen an den Daten seit der letzten vollständigen Datensicherung. Im Vergleich zu inkrementellen Datensicherungen benötigen differentielle Datensicherungen mehr Speicherplatz.

Für Unternehmen und Organisationen, die keine eigene IT-Abteilung oder keine ausreichenden Ressourcen für die Datensicherung haben, gibt es **externe Dienstleister**, die Datensicherungs- und Wiederherstellungsdienste anbieten. Diese Dienstleister können den gesamten Prozess übernehmen und somit eine zusätzliche Sicherheitsschicht bieten. Darüber hinaus können sie auch helfen, die **Datensicherungsstrategie** des Unternehmens oder der Organisation zu entwickeln und umzusetzen.

Eine Datensicherung ist eine Art Lebensversicherung für den Geschäftsbetrieb. Daher sollte die **Zuverlässigkeit** der Speicherung oberste Priorität haben. Dabei ist neben anderen Aspekten in der Beschaffung auch die **Lieferkette von Hard- und Softwareprodukten** einzubeziehen, die für die Sicherung infrage kommen.

Welche Chancen gibt es?

Backups **schützen vor Datenverlust** durch versehentliches Löschen, Hardwarefehler oder Cyberangriffe. Durch die Wiederherstellung von Daten im Falle eines Datenverlusts können Unternehmen und Organisationen ihre **Geschäftskontinuität** sicherstellen.
Je nach Anforderungen können verschiedene Arten von Datensicherungen eingesetzt werden, um den Bedürfnissen des Unternehmens oder der Organisation gerecht zu werden. Die Methode kann **leicht skaliert** werden und dadurch an die wachsenden Anforderungen der jeweiligen Organisation angepasst werden. Letztlich können durch den Einsatz von Backups teure **Wiederherstellungsverfahren** oder Lösegeldzahlungen bei Ransomwarefällen vermieden werden, sollte es zu einem Cybervorfall kommen. Allerdings muss im Falle eines Ransomwarevorfalls die Datensicherung vor der Nutzung detailliert auf Viren geprüft werden und sollte demnach so weit zurückgehen, dass eine **nicht virusverseuchte Sicherung** vorhanden ist.

Welche Risiken gibt es?

Der Einsatz von Datensicherungen erfordert in der Regel zusätzliche Hardware und Software sowie gegebenenfalls externe Dienstleistungen, was mit **zusätzlichen Kosten** für Unternehmen und Organisationen verbunden ist. Sie benötigen ein gewisses Maß an **Fachwissen** und können für Unternehmen und Organisationen mit begrenzten IT-Ressourcen komplex sein.
Zudem können Backups auch **Sicherheitsrisiken** mit sich bringen, insbesondere wenn sie nicht ordnungsgemäß konfiguriert oder gehandhabt werden. Es ist zu empfehlen Datensicherungen in einem **eigenen Netzwerksegement** zu betreiben, damit ein potenzieller Angriff erschwert wird. Ein Angriff auf den Speicherort der Datensicherung kann ebenfalls zu einem Datenverlust führen.

Fazit

Insgesamt sind Datensicherungen ein wichtiger Bestandteil der Cybersicherheit für Unternehmen und Organisationen. Nutzer sollten sicherstellen, dass ihre **Datensicherungsstrategie angemessen konfiguriert** ist und die erforderlichen Sicherheitsvorkehrungen getroffen wurden, um das Risiko von Cyberangriffen zu minimieren.
Insgesamt ist ein zuverlässiges Backup ein wesentlicher Bestandteil zur **Sicherung der Geschäftskontinuität** und sollte daher als wichtiger Aspekt des **Risikomanagements** behandelt werden.

Cyber-Sicherheitsrat Deutschland e.V.