Suisse Cyber Security

So schützen Sie sich vor Datenverlust...

(ein Suisse Cyber Security InHouse- Interview mit ICT- Forensiker und SCSC Jens B.)

Egal ob ein Verschlüsselungsvirus zuschlägt oder die Festplatte den Geist aufgibt: Datenverluste sind schwer zu verkraften.
Mit dieser Backup-Strategie sind Sie zu 99,9% sicher.

Eigentlich macht die Digitalisierung ihren Nutzern Leben und Arbeiten nur einfacher. Sämtliche Aufgaben gelingen schneller, effizienter und nehmen weniger Platz weg. Doch von einer Sekunde auf die Nächste kann diese perfekte Welt in sich zusammenstürzen. Plötzlich liegen Geschäftsemails, Kundenkontakte, digital gespeicherte Zugriffsdaten und Dokumente aller Art begraben in der Datenruine.

Plötzlich sind die Daten weg!

„Ein Stromausfall genügt, um die empfindlichen Schreib-/Leseköpfe der Festplatte zu zerstören und sie unbrauchbar zu machen", erklärt Senior Cyber Security Consultant Jens. Der ICT- Forensiker hat schon dutzenden Unternehmen geholfen, verlorene Daten wiederherzustellen. Das klappt in 95 Prozent der Fälle – selbst bei Feuer- und Wasserschäden.

Aber leider ist nicht immer eine Wiederherstellung der Daten möglich. Bestes Beispiel dafür sind die aktuell grassierenden Kryptoviren. Sie verschlüsseln die

Dateien auf den Festplatten infizierter Computer. Nur gegen Zahlung eines Lösegeldes geben Cyberkriminelle ihren Opfern dann den nötigen Schlüssel zur Wiederherstellung der Daten. „Allerdings lassen sich die Daten auch damit häufig nicht vollständig wiederherstellen", sagt Jens.

Einfache Sicherung ist schnell erledigt

Das einzige sichere Mittel gegen alle Datenverluste sind Backups. Ein Backup-System besteht aus mindestens einem externen Speichermedium, das von allen Arbeitsplätzen physisch getrennt ist und einer Backup-Software.

Eine tägliche oder wöchentliche Sicherung der Daten reicht laut Jens für die meisten kleineren KMU's aus, um gegen Datenverlust im Fall einer defekten Festplatte gewappnet zu sein.

Kryptoviren befallen auch Sicherungssysteme

Gegen Verschlüsselungstrojaner greift diese Sicherungsstrategie allerdings zu kurz. „Ein Kryptovirus verschlüsselt alle angeschlossenen Laufwerke", sagt Jens. Das heisst: Auch das Backup-System ist nicht vor einem Angriff der Schadsoftware sicher. Das ist umso gefährlicher, weil diese Viren sich erst zu erkennen geben, wenn sie ihre Aufgabe nach ein paar Tagen abgeschlossen haben. Ehe man den Schaden bemerkt, ist es schon zu spät.

Der Senior Cyber Security Consultant empfiehlt daher, ergänzend zum Backup im Tages- oder Wochenturnus jeden Monat eine weitere vollständige Sicherung auf einem zusätzlichen Speichermedium durchzuführen. So verliert man im Fall eines Angriffs maximal die letzten vier Wochen neuer Daten.
Zudem müssen nicht nur die Computer selbst, sondern auch die externen Backup- und Speichermedien unbedingt und regelmässig mit der aktuellsten Antivirensoftware auf Viren und andere digitale Schädlinge überprüft werden.

Der richtige Speicher für Ihre Backups

Das passende Speichermedium hängt vor allem vom gewünschten Komfort und der Anzahl der Arbeitsplätze im Unternehmen ab. „Auch schlanke Lösungen können wirkungsvoll sein", sagt Jens. „Für einen Einzelarbeitsplatz genügt im Grunde eine externe Festplatte, die nach jedem Backup wieder vom Computer getrennt wird."

NAS-Systeme

Komfortabler lässt sich die Sicherung bei Einzelarbeitsplätzen mit sogenannten netzgebundenen Speichern gestalten. NAS-Speicher werden solche Festplattensysteme mit Netzwerkanbindung genannt. Mit ihnen lassen sich Backups automatisiert durchführen, ohne das lästige manuelle Verbinden des externen Speichers mit dem Computer. Allerdings ist hier zu beachten: Wenn der NAS-Speicher permanent mit dem Computer verbunden ist, kann ein Kryptotrojaner auch ihn angreifen.

Sobald mehrere Computer in einem Server-Netzwerk miteinander verbunden sind, werden nicht länger die einzelnen Arbeitsplätze gesichert, sondern Backups direkt vom Server gemacht. „Dazu installiert man im Server (-schrank) ein zusätzliches Backup-Laufwerk oder richtet einen gesonderten Backup-Server im Unternehmen ein", sagt Jens.

Nicht jede Sicherung ist ein Backup

Wer zur Datensicherung auf die Raid-Methode vertraut, hat damit noch kein sicheres Backup. Raid bedeutet übersetzt: Redundante Anordnung kostengünstiger Festplatten. Dabei wird die Hauptfestplatte permanent auf weitere Festplatten gespiegelt. Und hier liegt das Problem der fehlenden Sicherung: Werden Daten vom Hauptspeichermedium gelöscht oder verschlüsselt, übernehmen die anderen Raid-Platten die Änderung sofort. Somit gehen die Daten auf allen Platten gleichzeitig verloren. Vor einem Defekt einer Festplatte schützt die Raid-Methode hingegen sehr gut. Denn die Sicherung enthält nicht nur alle Dateien, sondern auch sämtliche Programme, die zum Funktionieren des Rechners nötig sind.

Suisse Cyber Security

Grosse Schäden durch schlechte Rettung

Sind die Daten einmal verloren, ist eine Rettung häufig noch möglich. Doch auch hier ist Vorsicht angebracht: „Viele Nutzer machen den Fehler und versuchen, mit einem Datenrettungstool aus dem Internet ihre Daten zurückzubekommen", sagt Datenforensiker und Senior Cyber Security Consultant Jens. Das Problem: „Damit machen sie oft mehr kaputt als sie wiederherstellen und verursachen so einen endgültigen Verlust ihrer Daten." Wurden Dateien gelöscht, besteht zum Beispiel die Gefahr, dass sie bei der Installation neuer Tools und den Schreibvorgängen bei Computer-Neustarts endgültig überschrieben werden. Handelt es sich dagegen um einen Hardware-Fehler, kann sich der Schaden durch anhaltende Nutzung ausweiten. Jens rät daher dringend, die Datenrettung einem Fachmann zu überlassen.

Das gleiche Vorgehen empfiehlt er auch, wenn ein Backup einmal zur Wiederherstellung verlorener Daten in Anspruch genommen werden muss. Vor allem wenn es sich dabei nicht nur um einfache Dateisammlungen handelt. „Gerade umfangreiche Backups müssen in das neue System richtig integriert und ihre Dateien den frisch installierten Programmen zugewiesen werden", sagt Jens. „Da sollte man auf Fachkräfte zurückgreifen."

| JENS B. - SCSC (Senior Cyber Security Consultant) im Suisse Cyber Security InHouse- Interview mit:
| ROGER REINHARD
| CEO & CCSC (Chef Cyber Security Consultant)
| Suisse Cyber Security
| www.suissecybersecurity.ch