



Pressemitteilung

Schwerin, den 31. März 2026

World Backup Day – Achtung Daten sichern!

Am 31. März 2026 ist auch in diesem Jahr wieder World Backup Day. Er soll daran erinnern, digitale Fotos, Videos und Dokumente durch Sicherheitskopien zu sichern. Denn sowohl privat als auch beruflich sind Daten mehr denn je zentraler Bestandteil des Alltags – und ihr Verlust mitunter folgeschwer.

„In Zeiten, in denen es immer wahrscheinlicher wird, von einer Cyberattacke betroffen zu sein, müssen wir als Gesellschaft insgesamt resilienter darauf reagieren können. Backups sind wesentlich, um den Schaden solcher Angriffe zu minimieren“, erklärt Sebastian Schmidt, der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern.

Für Unternehmen und Behörden sind Backups daher unverzichtbar. Mehr noch gehören sie zu den unternehmenskritischen Systemen, die essentiell für den Fortbestand und Erfolg sind. Die Datenschutz-Grundverordnung (DS-GVO) verpflichtet Unternehmen, personenbezogene Daten zu schützen, insbesondere zählt dazu auch die Absicherung vor Datenverlust (gem. Art. 32 DS-GVO). Häufig stellt bereits der bloße Verlust von personenbezogenen Daten eine meldepflichtige Datenpanne dar, selbst wenn damit kein unbefugter Zugriff durch Dritte verbunden ist. Wer personenbezogene Daten verarbeiten darf, muss auch sicherstellen, dass diese richtig, aktuell und verfügbar sind. Deshalb ist es hier unerlässlich, klare Backup-Strategien festzulegen, die Zugriffe abzusichern und auch regelmäßig zu testen, ob die Daten aus dem Backup tatsächlich wiederhergestellt werden können.

Aber auch Bürgerinnen und Bürger sollten ihre Daten regelmäßig sichern. Das Handy fällt herunter oder wird gestohlen. Der Computer verabschiedet sich. Auf einmal sind alle Fotos und damit auch die digitalen Erinnerungen sowie wichtige gespeicherten Dokumente und Unterlagen verschwunden, im schlimmsten Fall für immer. Liegt ein funktionierendes Backup, d.h. eine Sicherheitskopie auf einem anderen Speicherort vor, bleiben die Folgen des Datenverlustes überschaubar und bestenfalls unbedeutend. Empfehlenswert ist, Daten regelmäßig auf einem externen Datenträger wie einem USB-Stick oder einer externen Festplatte abzuspeichern. Diese sollten dann mindestens mit einem Passwort geschützt und bestenfalls verschlüsselt werden. Damit es am Ende kein böses Erwachen gibt, sollten diese Backups auch regelmäßig auf ihre Funktionsfähigkeit geprüft werden. Die Nutzung von Cloud-Diensten ist zwar praktisch und weit verbreitet, allerdings muss man sich dabei auch bewusst sein, dass die eigenen Daten auf fremden Servern irgendwo auf der Welt liegen können und damit potentiell ein Zugriff durch Dritte möglich ist. Wichtig ist daher eine sorgfältige Auswahl des Cloud-Dienstes, idealerweise in der EU, bei dem die Daten verschlüsselt aufbewahrt werden. Zudem sollte für die Anmeldung an diesem System eine 2-Faktor-Authentifizierung vorgesehen sein, da das Passwort alleine nicht ausreichend ist.

Weitere Informationen unter:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datensicherung-und-Datenverlust/datensicherung-und-datenverlust_node.html

Kontakt: presse@datenschutz-mv.de

Telefon: 0385 59494-37