

Verfügbarkeitskontrolle – ein dehnbarer Begriff?

Das siebte Gebot: Die Verfügbarkeitskontrolle

Neben fachgerechter und regelmäßiger Datensicherung gehören auch Virenschutzmaßnahmen und ein Notfallplan zur Verfügbarkeitskontrolle. Verlassen Sie sich dabei nicht zu sehr auf die DV-Verantwortlichen: Die IT führt erfahrungsgemäß kaum regelmäßige Prüfungen der Sicherungen und Rücksicherbarkeit durch. Nicht selten finden Sie als Datenschutzbeauftragter Schwachstellen im Konzept – sofern ein solches überhaupt vorhanden ist!

Das Bundesdatenschutzgesetz lässt wie üblich freien Spielraum in der Interpretation seiner Vorgaben. Hier heißt es zur Verfügbarkeitskontrolle lediglich, dass zu gewährleisten ist, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Zunächst gilt auch hier grundsätzlich, dass die erforderlichen Maßnahmen nach § 9 Satz 2 BDSG verhältnismäßig zum jeweils angestrebten Schutzzweck sein dürfen.

Definition der Schutzmaßnahmen über Dateiregister?

Um die erforderlichen Schutzmaßnahmen exakt definieren zu können, wäre ein Dateiregister erforderlich. „Alte Hasen“ im Datenschutz können sich noch daran erinnern, dass die BDSG-Novellierung aus dem Jahr 2001 die Verpflichtung zur Führung entsprechender Übersichten aufhob.

Es gab wohl kaum ein Unternehmen in Deutschland, dem es wirklich gelungen war, in sinnvoller Form ein Dateiregister zu führen und noch dazu aktuell zu halten ...

Ableitung aus Verfahrensübersichten?

Als Datenschutzbeauftragter bleiben Ihnen zur Definition des Schutzzwecks lediglich die zur Verfügung gestellten (oder selbst erstellten) Verfahrensübersichten. Jedoch stellt die Fülle der Verfahren mit beteiligten Systemen

und Prozessen eine hohe Anforderung an eine definierbare Transparenz.

Eine Herleitung des erforderlichen Schutzzwecks und die Definition der daraus abgeleiteten Verfügbarkeitsmaßnahmen gleichen daher einer Sisyphusarbeit.



Backups gehören zu den wichtigsten Maßnahmen, um die Verfügbarkeit zu garantieren

Beschränken Sie sich am besten auf die Form der Datenhaltung

Wesentlich einfacher lassen sich die Maßnahmen zur Verfügbarkeitskontrolle über die Form der Datenhaltung festlegen. Im Kern der BDSG-Forderung zum Gebot der Verfügbarkeitskontrolle geht es nämlich ausschließlich darum, Zerstörung oder Verlust von Daten zu unterbinden – also die physisch gespeicherten personenbezogenen Daten zu schützen.

Erstellen Sie eine Übersicht aller relevanten Speichermedien

Zuerst müssen Sie klären, auf welchen Endgeräten und Medien personenbezogene Daten gehalten werden. Verschaffen Sie sich eine Übersicht über:

- **Verwendete Server:** Nehmen Sie hierbei nicht nur die reale Hardware, sondern auch virtuelle Server in Ihre Aufstellung auf.
- **Speichermedien:** Network Attached Storage (NAS), die als unabhängige Speicherkapazität in einem Netzwerk eingesetzt werden
- **Mobile Datenträger:** USB-Sticks oder -Festplatten sowie Disketten, CD-ROM oder DVD, Backup-Medien wie Sicherungstapes, Videobänder aus Überwachungskameras
- **Weitere Mobilgeräte:** z.B. Note- oder Netbooks, auf denen personenbezogene Daten gespeichert werden, zudem können auch iPhone, Blackberry etc. betroffen sein
- **Web-Provider:** Daten beim Webdienstleister, z.B. im Shop-System
- **Cloud Computing:** Vergessen Sie keinesfalls die Daten in der „Cloud“, sofern entsprechende Anwendungen existieren.

Notfallvorsorge und Backup sind in manchen Unternehmen Fremdwörter

Anzunehmen wäre, dass die DV-Verantwortlichen sich um ein regelmäßiges Backup kümmern, um bei eventuellem Datenverlust eine schnelle Wiederherstellung zu ermöglichen. Doch weit gefehlt – entsprechend einer Studie gilt für erschreckende 40 % der kleinen und mittleren Unternehmen (KMU), dass der Schutz gegen Datenverlust keine Priorität hat.

Sollte auch in Ihrem Unternehmen die Notfallvorsorge ein Fremdwort sein, besteht zwingender Handlungsbedarf.

Checken Sie den Backup-Plan

Zu Ihren Kontrollmaßnahmen als Datenschutzbeauftragter gehört ein

Check der Backupmaßnahmen. Prüfen Sie anhand Ihrer Übersicht der Speichermedien (s.o.), ob analog dazu ein regelmäßiges Backupverfahren existiert. Wichtigste Kriterien sind dabei:

- Wird eine Datensicherung durchgeführt?
- Sind die Backupintervalle der Sensibilität der zu sichernden Daten angemessen?
- Wird das Ergebnis der Sicherung regelmäßig überprüft (erfolgreich, abgebrochen, Fehlermeldungen)?
- Wo erfolgt die Lagerung der Sicherungsmedien?

Überprüfen Sie die organisatorischen Maßnahmen

Nicht auslassen dürfen Sie, eventuell organisatorische Maßnahmen zu kontrollieren. Was passiert beispielsweise im Urlaubsfall des Backup-Operators – ist für Stellvertretung gesorgt, um die Aufgaben (Tapewechsel, Einlagerung im Datensafe usw.) und die Ergebniskontrolle adäquat weiterzuführen? Oder passiert hier nichts?

Die Grundsicherungsmaßnahmen zur Verfügbarkeit

Verhindern Sie möglichen Datenverlust bereits durch den Einsatz entsprechender Grund- und Standardmaßnahmen:

1. Einbruchvorsorge und Diebstahlschutz
2. geeignete Brandschutzmaßnahmen
3. Schutz vor Stromausfall mittels USV-Anlagen
4. Vermeidung von Wasserschäden oder Vandalismus (geeigneter Serverraum)
5. Ausfallschutz durch Redundanz kritischer Anwendungen
6. Einsatz von RAID-Verfahren zur Datenspeicherung
7. Organisation der Datenhaltung (grundsätzlich auf Servern)
8. geeigneter Virenschutz und Firewallkonzept

Schauen Sie sich die Wiederherstellungsverfahren an

Was nützt die beste Datensicherung, wenn nicht für geeignete Maßnahmen zur schnellen Wiederherstellung bei Schadensfällen gesorgt ist? Entsprechende Notfallpläne und Handlungsanleitungen müssen zwingend vorhanden sein. Dabei bergen Daten in der Cloud oftmals besondere Herausforderungen an Restoremaßnahmen.

Achten Sie auf die K.-o.-Kriterien

Verlassen Sie sich bitte nie auf die Aussagen der IT-Verantwortlichen, dass eine Wiederherstellung verloren gegangener oder aus Versehen gelöschter Daten jederzeit möglich wäre. In der Regel sind Restoreverfahren äußerst selten bis nie geprüft oder scheitern wegen mangelnder Vorbereitung bzw. unzureichender Dokumentation.

K.-o.-Kriterien sind:

- fehlende Sicherungsmedien (bei ungeordneter oder fehlender/unzureichender Kennzeichnung)
- defekte Sicherungsmedien (überaltertes Medium)
- nicht bekanntes Passwort bei kennwortgeschützten Sicherungsdatenträgern
- Unkenntnis des Bedieners zum Restoreablauf („Hab‘ ich noch nie gemacht.“)
- mangelnde Kenntnis zur Datenintegrität (Zusammenhänge mit anderen Dateien oder Anwendungen)

Fragen Sie unbedingt nach dem aktuellen Notfallplan

Zur Notfallvorsorge muss eine aussagekräftige und für IT-Mitarbeiter nachvollziehbare Dokumentation vorliegen. Die Verfügbarkeitsplanung darf nicht erst nach einem Ausfall oder einem Datenverlust in Angriff genommen werden.

Idealerweise gehört zu einem funktionierenden Notfallplan eine regelmäßige

Weiterführende Informationen

Wie steht es wirklich um Ihre Datenverfügbarkeit? Lesen Sie mehr dazu in einem Beitrag von Oliver Schonschek unter www.datenschutz-praxis.de/fachwissen/fachartikel/wie-steht-es-wirklich-um-ihre-datenverfugbarkeit

Test-Rücksicherung mit wechselndem Personal. Nur wenn der Ernstfall über regelmäßige Testszenarien regelmäßig geprobt wird, lassen sich im Schadensfall die schadhafte Daten wirkungsvoll wiederherstellen.

Datenverlust sollte zumindest mit der Grundsicherung vorgebeugt sein

Eine Datenwiederherstellung sollte immer letztes Mittel einer gesicherten Verfügbarkeitskontrolle sein. Um Informationen gegen zufällige Zerstörung oder Verlust zu schützen, empfiehlt es sich, vorbeugende Maßnahmen zur Datensicherung einzusetzen.

Zu einer angemessenen Grundsicherung, nicht nur von personenbezogenen Daten, sondern generell für alle geschäftsrelevanten Informationen, stehen ausreichende technische und organisatorische Mittel zur Verfügung (siehe Kasten zur Grundsicherung).

Holen Sie die Geschäftsleitung ins Boot

Sofern Sie bei Ihrer Prüfung zur Verfügbarkeitskontrolle feststellen, dass die aktuellen Maßnahmen ungenügend bis nicht ausreichend sind, sollten Sie unbedingt die Geschäftsleitung informieren.

Ein Systemausfall oder Datenverlust kostet ein KMU durchschnittlich einen oberen vierstelligen Eurobetrag. Ein Grund mehr, die Datenverfügbarkeit ernst zu nehmen!

Hermann Keck

Hermann Keck ist externer Datenschutzbeauftragter (www.keck-dsb.de).