ALTE LEIPZIGER
Versicherung Aktiengesellschaft

Vertragsbestandteil T 128.1
Erläuterungen zu Ziffer 7.1.5 der VHV laufende Versicherung 2003/2011

Fassung Januar 2018

Die nachfolgenden Erläuterungen stellen beispielhaft Maßnahmen zu Schutz und Sicherung informationsverarbeitender Systeme dar. Die konkrete Ausgestaltung der einzelnen Maßnahmen obliegt dem Versicherungsnehmer und sollte unter Berücksichtigung der Größe des Betriebes und des Umfangs der IT-Nutzung erfolgen. Das bedeutet, dass auch andere oder weiterreichende Maßnahmen erforderlich sein können, um der gemäß Ziffer 7.1.5 vereinbarten Obliegenheit zu entsprechen.

1. Schutz vor unberechtigten Zugriffen

1.1 Die informationsverarbeitenden Systeme sollen einzelne Nutzer und Befugnisebenen unterscheiden. Hierzu sind individuelle Zugänge für alle Nutzer erforderlich, die mit Passwörtern angemessen gesichert werden, die möglichst aus einer Zeichenkombination aus Buchstaben, Zahlen und Sonderzeichen unter Verwendung von Groß- und Kleinschreibung bestehen sollten. Administrative Zugänge sind ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten.

Sie sollen darüber hinaus mit einem zusätzlichen Schutz gegen unberechtigten Zugriff ausgerüstet sein, wenn sie einem erhöhten Risiko ausgesetzt sind. Ein erhöhtes Risiko besteht bei Geräten, die über das Internet erreichbar oder im mobilen Einsatz sind.

Zusätzliche Schutzmaßnahmen können z. B. sein: Firewall, 2-Faktor-Authentifizierung bei Servern, Verschlüsselung von Datenträgern mobiler Geräte, Diebstahlsicherung oder ähnlich wirksame Maßnahmen

2. Sicherung und Schutz der Daten

2.1 Die Systeme sollen einem Patch-Management-Verfahren unterliegen, das eine zeitnahe Installation von relevanten Sicherheitspatches sicherstellt. Systeme und Anwendungen mit bekannten Sicherheitslücken dürfen nicht ohne zusätzliche Maßnahmen zur Absicherung eingesetzt werden.

Soweit nichts anders vereinbart ist, sollen die Systeme einem mindestens wöchentlichen Sicherungsprozess unterliegen, wobei die Sicherungsdatenträger physisch getrennt aufbewahrt werden, um sicher zu stellen, dass im Versicherungsfall auf Originale und Duplikate nicht gleichzeitig zugegriffen oder diese manipuliert oder zerstört werden können.

Die Systeme sind ausreichend vor Beschädigung oder Störung durch berechtigte Nutzer zu schützen, zum Beispiel durch Regelungen zur privaten Nutzung und zum Gebrauch von Datenträgern und Software sowie Schulungen zur IT-Sicherheit.

3. Laufende Kontrolle

Der Versicherungsnehmer hat eine ordnungsgemäße Funktion des Sicherungs- und Wiederherstellungsprozesses durch regelmäßige Prüfung nach einem festgelegten Turnus sicherzustellen.

4. aktueller Stand der Technik

Die eingesetzten Systeme müssen dem aktuellen Stand der Technik entsprechen, in der aktuellen Version vorgehalten werden und für eine gewerbliche Nutzung zugelassen sein.

Der Versicherungsnehmer hat die in Ziffer 7.1.5 genannte Obliegenheit auch im Falle einer Beauftragung externer Dienstleister zu beachten.