ALTE LEIPZIGER
Versicherung Aktiengesellschaft

Vertragsbestandteil C 02.2

Obliegenheiten vor Eintritt des Versicherungsfalls zur Gewährleistung der IT-Sicherheit

Fassung Juni 2022

	IT-Sicherheitsvereinbarung	Erläuterungen und Empfehlungen
Zugriffssicherung	Die informationsverarbeitenden Systeme unterscheiden einzelne **Nutzer und Befugnisebenen**. Hierzu sind individuelle und mit einem **Passwort** gesicherte Zugänge für alle Nutzer vorhanden. Wird vom Versicherungsnehmer ein **WLAN für betriebsfremde Personen** (z. B. Gäste-WLAN) zur Verfügung gestellt, ist dieses ebenfalls mit einem Passwort gesichert und vom restlichen Unternehmensnetzwerk getrennt.	Nutzer und Befugnisebenen Der Zugang zu relevanten Teilen der Infrastruktur wird über Passwörter geschützt. Darüber hinaus sind unterschiedliche Berechtigungen über Benutzergruppen oder einzelne Benutzer zu vergeben. Dies bezieht sich nicht nur auf den Dateizugriff, sondern auch auf die Administration einzelner Bereiche der Infrastruktur. Es ist darauf zu achten, dass User-Accounts keine administrativen Berechtigungen erhalten. Dies darf selbst dann nicht der Fall sein, wenn ein Zugreifender gleichermaßen Administrator und Benutzer ist. Dieser hat sich dann – abhängig von der anliegenden Aufgabe – entweder mit dem Administrator-Account oder mit dem normalen User-Account einzuloggen. Passwörter Passwörter regeln den Zugriff auf unterschiedliche Bereiche der Infrastruktur und beschränken ggf. den Zugriff auf Daten. Passwörter müssen mindestens 8 Zeichen lang sein sowie aus einer Kombination aus Groß- und Kleinbuchstaben, mehreren Ziffern sowie Sonderzeichen bestehen. Neben einem Passwort oder anstelle dessen können auch biometrische Verfahren genutzt werden. Die Passwortrichtlinie gilt ebenfalls für mobile Geräte (Notebooks, Handys und Tablets) und für eine Anmeldung an einem Virtual Private Network (kurz: VPN). **Es wird empfohlen**, eine 2-Faktor-Authentisierung für die Anmeldung an das lokale Netz sowie an das VPN einzurichten. Es ist darauf zu achten, dass die vom System vorgegebenen Konten deaktiviert werden und durch eigene und individualisierte Konten mit gleichen Berechtigungen ersetzt werden (soweit möglich). Für Administrator-Accounts ist eine einfache PIN-Authentisierung grundsätzlich nicht ausreichend. Der Versicherungsnehmer kann aber in begründeten Ausnahmefällen diese anwenden, sofern für ihn eine andere Lösung hinsichtlich der Aufwände nicht zumutbar wäre. Dies ist entsprechend durch den Versicherungsnehmer zu dokumentieren. WLAN für betriebsfremde Personen Ein Router verbindet die Infrastruktur mit dem Internet. Er stellt außerdem eine Drahtlosverbindung sowohl mit dem Internet, als auch mit den eigenen Netzwerkressourcen her. Der Router betreibt den Adressbereich des lokalen Netzwerks durch Network Address Translation (kurz: NAT). Er stellt außerdem WPA2-/WPA3-verschlüsselte Drahtlosverbindungen zur Verfügung. **Es wird empfohlen**, bei einem neueren Sicherheitsstandard diesen so schnell wie möglich zu etablieren. Stellt der Router explizit ein WLAN für betriebsfremde Personen (z. B. Gäste-WLAN) zur Verfügung, ist darauf zu achten, dass dieses Netzwerk komplett vom Unternehmensnetzwerk getrennt ist. **Es wird empfohlen**, den betriebsfremden Personen individuelle Zugänge zur Verfügung zu stellen (Einmal-Voucher) sowie auch die Bandbreite zu beschränken. Optional unterliegen die Zugänge auch einer inhaltlichen Kontrolle. Darüber hinaus sind die Nutzer über die jeweils aktuellen gesetzlichen Vorschriften im Hinblick auf IT-Sicherheit und Datenschutz zu informieren und es sollte ihr Einverständnis zur Einhaltung der Nutzungs-vorschriften über einen Check-Button bestätigt werden.

	IT-Sicherheitsvereinbarung	Erläuterungen und Empfehlungen
Zugriffssicherung	Die informationsverarbeitenden Systeme sind mit einem **zusätzlichen Schutz** gegen unberechtigten Zugriff ausgerüstet und **zertifikatsbasiert verschlüsselt**, wenn diese über das Internet erreichbar oder im mobilen Einsatz sind.	Zusätzlicher Schutz gegen unberechtigte Zugriffe Die Infrastruktur muss durch eine Firewall nach außen hin Richtung Internet abgeschottet sein. Diese muss gemäß den Herstellervorgaben so konfiguriert sein, dass nur der erforderliche Netzwerkverkehr zugelassen wird (in beide Richtungen). **Es wird empfohlen**, diese Server täglich auf Vorfälle zu untersuchen und mit den aktuellen Patches zu versehen. Daten, die auf mobilen Geräten (Notebooks, Handys und Tablets) verwendet werden, müssen auf verschlüsselten Partitionen/Festplatten gespeichert werden. Darüber hinaus hat sich jeder Benutzer des Systems über ein Passwort zu authentifizieren. **Es wird empfohlen**, dass Handys und Tablets über eine Vorrichtung verfügen, die es ermöglicht, sämtliche Inhalte aus der Ferne zu löschen. Zertifikatsbasierte Verschlüsselung Bei der zertifikatsbasierten Verschlüsselung kommen innerhalb einer Sicherheitsinfrastruktur, der sogenannten Public-Key-Infrastruktur (PKI), digitale Zertifikate zur Anwendung, um einen sicheren Austausch von Daten zwischen Kommunikationspartnern im Internet zu gewährleisten. Das digitale Zertifikat ist ein elektronischer Echtheitsnachweis, der von einer Zertifizierungsstelle ausgestellt wird und die vergleichbare Funktion eines Personalausweises besitzt.
Datenversand	Werden **besonders schützenswerte Daten** (u. a. besondere Kategorien personenbezogener Daten gemäß **DSGVO**) Dritter über das Internet versendet, so sind diese Daten **verschlüsselt.**	Besonders schützenswerte Daten Unter besonders schützenswerte Daten fallen z. B. ■ Gesundheitsdaten, ■ Geschäftsgeheimnisse oder ■ Finanz- und Steuerdaten. DSGVO Unter DSGVO wird die Datenschutz-Grundverordnung verstanden. In Artikel 9 DSGVO werden besondere Kategorien personenbezogener Daten beschrieben. Verschlüsselter Datenversand Besonders schützenswerte Daten werden nur verschlüsselt entsprechend den geltenden Datenschutzbestimmungen versendet oder weiterverarbeitet. Abzugrenzen von besonders schützenswerten Daten sind personenbezogene Daten (z. B. Telefonnummer, Kontodaten, Kfz-Kennzeichen). **Es wird empfohlen,** diese personenbezogenen Daten entsprechend den geltenden Datenschutzbestimmungen anonymisiert zu versenden oder weiterzuverarbeiten bzw. bei Versand oder Verarbeitung in einer Cloud zu verschlüsseln.
Schutz vor Schadsoftware	Die informationsverarbeitenden Systeme verfügen über einen Schutz gegen **Schadsoftware**, die sich automatisch aktualisiert.	Schadsoftware Die einzelnen Rechner und Nodes (Datenknotenpunkte) sind mit einer Endpoint-Security gegen Malware (Viren, Würmer und Trojaner) zu schützen. Die Lösung muss zentral administriert werden und in der Lage sein, sicherheitsrelevante Vorfälle anzuzeigen. Zudem ist die Lösung automatisch mit aktuellen Signaturen (für Viren, Würmer und Trojaner) zu versorgen. **Es wird empfohlen,** zusätzlich eine Lösung speziell gegen Ransomware zu installieren und zu pflegen. Die Endpoint-Security muss neben dem Virenschutz auch eine Client-Firewall bereitstellen, die auf sämtlichen Clients zu installieren und zu aktivieren ist. **Es wird empfohlen,** eine Device-Control zu installieren. Diese kontrolliert sämtliche Schnittstellen der einzelnen Rechner – insbesondere aber die USB-Ports. Die Device Control ist so zu konfigurieren, dass nur zugelassene USB- und Speichersticks zum Einsatz kommen dürfen. Darüber hinaus sollten auch Regeln für den Umfang und den Inhalt der zu kopierenden Daten definiert werden. **Es wird empfohlen,** eine Web Application Firewall (WAF) zu installieren, die applikationsbasierte Regeln zulässt. Idealerweise wird bereits auf der Firewall ein System zum Auffinden von Malware etabliert.

	IT-Sicherheitsvereinbarung	Erläuterungen und Empfehlungen
Sicherheitsupdates	Die informationsverarbeitenden Systeme unterliegen einem **Patch-Management-Verfahren**, das eine unverzügliche Installation (mindestens monatlich) relevanter Sicherheitspatches sicherstellt. Systeme und Anwendungen mit bekannten Sicherheitslücken dürfen nicht ohne zusätzliche geeignete Maßnahmen zur Absicherung eingesetzt werden.	Patch-Management-Verfahren Jedes System, das mit Software betrieben wird, muss in zyklischen Abständen gepatcht werden. Darunter versteht man die Aktualisierung sämtlicher Software auf den unterschiedlichen Systemen. Der Patch-Prozess muss – unabhängig ob Desktops, Notebooks, andere Mobilgeräte oder Server – monatlich durchgeführt werden und sämtliche sich im Betrieb befindliche Software umfassen. Systeme, die mit einer Software betrieben werden, die vom Hersteller nicht mehr unterstützt wird, dürfen nur noch in vom restlichen Netzwerk abgeschotteten Bereichen und ohne Internetverbindung genutzt werden. Dadurch soll verhindert werden, dass unter Ausnutzung einer bekannten und nicht mehr gepatchten Schwachstelle auf einem solchen System das gesamte Netzwerk zugänglich wird.
Datensicherung	Die informationsverarbeitenden Systeme unterliegen einem mindestens wöchentlichen **Sicherungsprozess**. Der **Sicherungsdatenträger** wird physisch getrennt aufbewahrt. Es ist sicherzustellen, dass im Versicherungsfall auf Originale und Duplikate nicht gleichzeitig zugegriffen werden kann oder diese manipuliert oder zerstört werden können. Einmal jährlich prüft der Versicherungsnehmer, ob der **Sicherungs- und Wiederherstellungsprozess** ordnungsgemäß funktioniert.	Sicherungsprozess Sowohl erfasste Daten als auch Programm- und Konfigurationsdaten müssen zyklisch gesichert werden. Der Datensicherungsprozess beinhaltet nicht nur die reinen Daten, sondern auch die Systemumgebung der gesamten Infrastruktur und Konfigurationsdaten sämtlicher Geräte und Lösungen. Datensicherungen sind so durchzuführen, dass ein Zurückspielen der Daten jederzeit komplett oder selektiv möglich ist. Es ist darauf zu achten, dass Programm-, System- und Konfigurationsdaten so gesichert werden, dass eine Rücksicherung bei System-Komplettausfällen schnell und effizient zu einer vollständigen Systemwiederherstellung und damit zur Herstellung der Produktivität führen. Rohdaten müssen entsprechend ihres Formates applikationsgerecht gesichert werden. **Es wird empfohlen**, eine tägliche Sicherung anzustoßen und einmal pro Woche eine Komplettsicherung durchzuführen. Sicherungsdatenträger Die Sicherung kann sowohl lokal als auch in der Cloud durchgeführt werden. **Es wird empfohlen**, bei einer Sicherung in der Cloud vor dem Transfer der Daten zum Provider diese zu verschlüsseln. Werden die Daten lokal gesichert, ist darauf zu achten, dass geeignete Datenträger verwendet werden. Diese zeichnen sich durch Manipulationssicherheit und Robustheit gegenüber Zeit, Markt und physikalischen Umgebungsveränderungen aus. Handelsübliche Datenträger erfüllen i. d. R. diese Anforderungen. Die Datenträger sind räumlich getrennt von der IT-Infrastruktur aufzubewahren. Sicherungs- und Wiederherstellungsprozess Der Wiederherstellungsprozess muss mindestens einmal pro Jahr, jedoch umgehend nach Einführung eines neuen Backup-Systems durchgeführt werden. In jedem Fall ist eine Dokumentation zu erstellen. Es ist sicherzustellen, dass sowohl Teilwiederherstellungen als auch Komplettrücksicherungen möglich sind. Dabei ist zu berücksichtigen, dass es möglich sein muss, Komplettsicherungen auch auf anderer (neuer) Hardware wiederherstellen zu können.
Dokumentation	Ab 5 Mio. EUR Jahresumsatz: Es existiert ein **IT-Notfall- und Wiederanlauf-Konzept (Notfallplan)**, welches schriftlich fixiert ist und Verantwortliche benannt hat.	IT-Notfall- und Wiederanlauf-Konzept (Notfallplan) Ein IT-Notfall- und Wiederanlauf-Konzept (Notfallplan) beinhaltet alle erforderlichen Schritte, Prozesse und Beschreibungen, um die Infrastruktur bei einem Total- oder Teilausfall wieder in einen produktiven Modus zu bringen. **Es wird empfohlen**, dass das Konzept mindestens Verantwortlichkeiten, Rollen und Prozesse, Ort und Zugang für Notfall-Accounts, Passwörter, Pläne zur Neuinstallation aller relevanten Produktiv-Systeme, eine Beschreibung der Hard- und Software sowie alle Dienstleister und Provider enthält. Das Notfallkonzept ist in ausgedruckter Form räumlich getrennt vom System aufzubewahren und dem System entsprechend zyklisch anzupassen.

	IT-Sicherheitsvereinbarung	Erläuterungen und Empfehlungen
Sicherheitsvorschriften	Alle **gesetzlichen, behördlichen** sowie vertraglich vereinbarten **Sicherheitsvorschriften** werden eingehalten.	Gesetzliche-, behördliche- und Sicherheitsvorschriften Es gelten die einschlägigen gesetzlichen Bestimmungen. Empfehlungen für Planung, Strukturierung und Administration von IT-Infrastrukturen sowie der aktuellen Sicherheitslage sind zu finden bei: ■ www.bitkom.org ■ www.bsi.de ■ www.vds.de
Allgemeine Regelung	Besonders gefahrdrohende Umstände werden auf Verlangen des Versicherers innerhalb angemessener Frist beseitigt. Dies gilt nicht, soweit die Beseitigung unter Abwägung der beiderseitigen Interessen unzumutbar ist. Ein Umstand, der zu einem Schaden geführt hat, gilt ohne weiteres als besonders gefahrdrohend.	