Erläuterungen zu den Risikofragen der Cyberversicherung

6.6 Mitarbeiter haben nur die Zugänge und Rechte, welche für die Erfüllung der Tätigkeiten erforderlich sind. Weitergehende Rechte
– sind ausschließlich Administratoren und zur Erledigung administrativer Tätigkeiten vorbehalten,
– werden regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft. 6

6.7 Die Installation von Sicherheits-Patches für unsere IT wird zentral gesteuert. 6

6.8 Es bestehen technische Mindestanforderungen an die Zugangspasswörter (min. 8 Zeichen; Zahlen und Buchstaben; Groß- und Kleinschreibung).
Kennwörter müssen in einem regelmäßigen Turnus geändert werden. 6

6.9 Es sind Vorkehrungen für einen IT-Notfall (Wiederanlaufkonzept) getroffen und Verantwortliche benannt. 6

1 Sicherheitsstandards:

Damit Cyberrisiken versicherbar sind, müssen bestimmte Mindestanforderungen durch den Versicherungsnehmer erfüllt werden. Daher muss der Versicherungsnehmer die Einhaltung dieser Standards durch die im Folgenden näher erläuterten Aussagen bestätigen, damit der Versicherungsvertrag geschlossen und aufrechterhalten werden kann.

1.1 Für den Zugang zu jedem System sind für jeden Nutzer und Administrator eine individuelle Benutzerkennung und ein Passwort notwendig.

Systeme ohne Authentifizierung können von Angreifern ohne Hindernis übernommen und kontrolliert werden. Daher sehen aktuelle Betriebssysteme grundsätzlich eine Authentifizierung vor. Benutzerindividuelle Kennungen sind darüber hinaus notwendig, um die Zugriffsrechte einzelner Accounts granular zu definieren und nachvollziehen zu können, welche angriffs- oder schadenrelevanten Tätigkeiten zu welchem Zeitpunkt von welchem Nutzer durchgeführt wurden. Sogenannte „Funktionsaccounts", also Log-in-Daten, die sich mehrere Personen teilen, dürfen nur an unkritischen Systemen und Software verwendet werden. Als kritisch werden administrative bzw. vollständige Änderungs- und Löschrechte auf sensible Personendaten (Datenschutz) oder IT-Infrastruktur (z. B. Server) angesehen.
Zudem ist sicherzustellen, dass in den Betriebssystemen je Nutzer eigene Konten angelegt/genutzt werden. (z. B. Windowskonto)

1.2 Alle informationsverarbeitenden Systeme verfügen über einen Schutz gegen Schadsoftware.

Informationsverarbeitende Systeme sind sämtliche von den Versicherten selbst betriebene und beruflich genutzte Hardware- und Softwaresysteme einschließlich Netzwerkkomponenten und Netzwerken sowie Endgeräten (auch mobile). Auf diesen Systemen ist ein Schutz gegen Schadsoftware zu installieren. Hierzu zählen alle handelsüblichen Anti-Viren-Programme inkl. einer betriebssystemeigenen Schutzsoftware, sofern es sich um die aktuellste Version des Betriebssystems handelt und eine automatische Aktualisierung des Anti-Virenprogramms und Betriebssystems sichergestellt ist.

1.3 Geräte, die über das Internet erreichbar sind, haben wir mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen.

Server oder Geräte, die mit dem Internet direkt oder indirekt verbunden sind, sind dort einem allgemeinen und ständigen Angriffsrisiko ausgesetzt und unterliegen daher höheren Schutzanforderungen als stationäre Bürorechner.

Zu den erforderlichen Maßnahmen können gehören:
– Firewall-Software
Es handelt sich hierbei um eine Software, welche den Netzwerkzugriff überwacht und unerlaubte Fernzugriffe auf ein Netzwerk verhindern soll. Ausreichend für die positive Beantwortung dieser Frage ist, wenn eine Personal-/Desktop-Firewall auf allen mit dem Internet verbundenen Geräten installiert, aktiviert und laufend aktualisiert wird.
Die Windows-eigene Firewall ist hierfür nicht ausreichend.

– Zwei-Faktor-Authentifizierung
Möglichkeit der Authentifizierung durch zwei unterschiedliche und unabhängige Faktoren (Komponenten)
Beispiel: Zugangskarte (Chipkarte) in Verbindung mit einem Kennwort
Kennwort in Verbindung mit automatisch generierter PIN auf Mobiltelefon

– Zertifikatsbasierte Anmeldung
Auf dem System gespeicherte Zertifikate werden genutzt, um einen Benutzer zweifelsfrei auszuweisen.

– Security Monitoring und Intrusion Detection System
Netzwerk- oder Security Monitoring ist ein Teil des Netzwerkmanagements.
Unter Netzwerk-Monitoring versteht man die Überwachung und die regelmäßige Kontrolle von Netzwerken, deren Hardware (z. B. Server, Router, Switches) und Dienste (z. B. Webserver, DNS-Dienste, E-Mail-Dienste).

Ein Intrusion Detection System ist eine sinnvolle Ergänzung einer bestehenden Firewall, kann aber auch direkt auf einem zu überwachenden System eingesetzt werden. Es dient der Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind und kann so die Sicherheit von Netzwerken und Computersystemen erhöhen. Erkannte Angriffe werden meistens in Log-Dateien gespeichert und dem Benutzer oder Administrator mitgeteilt.

– oder ähnliche Maßnahmen, die einen Fernzugriff erschweren.

1.4 Wir stellen sicher, dass alle Systeme und sicherheitsrelevante Standardsoftware auf aktuellem Stand sind und installieren Sicherheitsupdates automatisch oder zeitnah.

Mit der Veröffentlichung von Sicherheitsupdates werden auch die zugrunde liegenden Software-Schwachstellen der allgemeinen Öffentlichkeit bekannt. Dadurch steigt das Risiko des Betriebs nicht aktueller Software. Besonderes Augenmerk ist dabei auf verwendete Standardsoftware zu legen. Hierzu zählen u. a. Adobe Reader, Internetbrowser, MS Office.

In besonders geschäftskritischen Bereichen ist es üblich, Updates zunächst einer Prüfung zu unterziehen, um Probleme im Betrieb auszuschließen. In diesem Fall ist anstelle eines automatischen Updates ein zeitnahes Umsetzen je nach Kritikalität des Updates angemessen.

1.5 Wir schützen uns vor dem Verlust der Unternehmensdaten durch mindestens wöchentliche Datensicherung.
Ohne Datensicherung ist eine Wiederherstellung der Betriebsbereitschaft kaum möglich. Ein nachhaltiger Datenverlust bedeutet darüber hinaus nicht selten eine lang dauernde Betriebsunterbrechung. Unter einer wöchentlichen Datensicherung verstehen wir die mindestens im Wochenabstand erfolgende Sicherung aller Daten (Vollsicherung). Es empfiehlt sich, sensible Daten zusätzlich öfter zu sichern.

1.6 Die Datensicherungsmedien werden
– physisch getrennt von den gesicherten Systemen aufbewahrt und
– vor unberechtigtem Zugriff sowie nachträglicher Manipulation geschützt.
Wenn Backup-Systeme dauerhaft mit den Zielsystemen verbunden sind, besteht das Risiko, dass sie bei einem Angriff ebenfalls zu Schaden kommen. Daher sind diese an einem geschützten Ort und ohne Netzzugriff aufzubewahren.
Wenn Back-ups nachträglich vom betroffenen System oder vor dem Angreifer verändert werden können, besteht das Risiko, dass sie ebenfalls zu Schaden kommen.

1.7 Wir stellen durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass unsere Datensicherung und -wiederherstellung funktionieren.
Eine regelmäßige Überprüfung der Wiederherstellung stellt sicher, dass diese auch im Ernstfall vollständig funktioniert. Findet eine solche regelmäßige Prüfung nicht statt, sind aufgrund des unerprobten Vorgangs Probleme durch Unvollständigkeit oder Verzögerungen bei der Wiederherstellung wahrscheinlicher.
Die Lebensdauer eines Datenträgers ist begrenzt. Ebenso können Systemausfälle oder andere Gründe dazu führen, dass Daten nicht ordnungsgemäß dupliziert wurden. Der Überprüfungs-Turnus richtet sich dabei nach Art und Häufigkeit der Sicherung und liegt zwischen 1 und 3 Monaten.

2 Sofern die Nutzung privater Geräte in Ihrer Unternehmens-IT gestattet ist:

2.1 Private Geräte befinden sich in einem separaten Netzwerksegment und haben keinen administrativen Zugriff auf geschäftliche Dienste oder Infrastruktur.
Mit Netzwerksegmentierung wird die Trennung oder Isolation von Netzwerken bezeichnet. Dies kann sowohl mithilfe von einer oder mehreren Firewalls oder durch physisch getrennte Netzwerke (z. B. separate WLAN-Netze) erreicht werden.
Aus Gründen der Sicherheit haben sie keine Verbindung mit anderen Netzwerken oder dem Internet.

Vorteile einer solchen Netzwerksegmentierung sind u. a.:
– Hohes Schutzniveau für unternehmenskritische Server und Applikationen auf einem Need-to-know-Prinzip (man muss Kenntnisse über deren Existenz haben).
– Gewährt nur legitimierten Mitarbeitern Zugriff auf die benötigten Netzwerkbereiche.
– Vereinfacht das Netzwerkmanagement. Dazu gehören auch das Ereignis-Monitoring und die Reaktion auf Vorfälle.
Beispiel für zu separierende Netze sind Warenwirtschaft, Kundendatenbank, Personalwirtschaft.

2.2 Die Nutzung ist vertraglich geregelt.
Da private Geräte nicht zentral gewartet werden, kann nicht sichergestellt werden, dass diese das definierte Sicherheitsniveau einhalten. Daher ist die Nutzung schriftlich zu regeln, z. B. in Form einer Betriebsvereinbarung, arbeitsvertraglichen bzw. individuellen Vereinbarung.

3 Wir nutzen einen Dienstleister zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten.
Durch Nutzung eines Dienstleisters gibt man die direkte Kontrolle über Daten, für die man verantwortlich ist, aus der Hand. Daher sind folgende weitere Voraussetzungen einzuhalten.

3.1 Es existiert ein Dienstleistungsvertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind.
Durch fehlende Verfügbarkeit, fehlende Updates und bestehende Sicherheitslücken besteht ein erhöhtes Ausfallrisiko des Dienstleisters.

3.2 Unser Dienstleister ist zertifiziert oder wir unternehmen regelmäßig eine unabhängige Qualitätssicherung.
Übliche Zertifizierungen für diesen Bereich sind VdS 3473, ISO 27001 und der BSI-Grundschutz.

3.3 Unser Dienstleister unterliegt dem einheitlichen Datenschutzrecht der Europäischen Union.
Eine Speicherung von Daten außerhalb des Anwendungsbereichs des europäischen Datenschutzrechts durch einen Dienstleister (Cloud-Anbieter) kann möglicherweise einen datenschutzrechtlichen Verstoß darstellen.

4 Es werden pro Jahr (einschließlich aller rechnergestützten Geräte und Computer) weniger als 20.000 Kreditkartendaten bearbeitet, gespeichert oder übermittelt?

Das Speichern von Kreditkartendaten unterliegt den Bedingungen des PCI-DSS. Der Payment Card Industry Data Security Standard ist ein Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht und von allen wichtigen Kreditkartenorganisationen unterstützt wird.

5 Unser Geschäftsmodell ist teilweise oder vollständig onlinebasiert.

Ein Teil des Umsatzes wird aus Onlinegeschäften erzielt.

5.1 Wir nutzen Dienstleister zum Betrieb unseres Webshops.

Spezialisierte Dienstleister können oft kürzere Wartungsintervalle und ein höheres allgemeines Sicherheitsniveau gewährleisten.

5.2 Wir nutzen einen Payment-Dienstleister zur Abwicklung aller eingehenden bargeldlosen Zahlungsvorgänge.

Spezialisierte Dienstleister können oft ein höheres allgemeines Sicherheitsniveau und ein geringeres Ausfallrisiko gewährleisten.

6 Wir verarbeiten oder speichern
– Daten, die besonderen gesetzlichen Verschwiegenheitspflichten unterliegen (z. B. Gesundheitsdaten),
– Geschäftsgeheimnisse oder Finanz- oder Steuerdaten von Dritten.

Das Speichern und Verarbeiten besonders sensibler Daten unterliegt besonderen Voraussetzungen an den Datenschutz. Eine unrechtmäßige Übermittlung oder Kenntnisgabe der in Betracht kommenden Daten löst in vielen Fällen Informationspflichten der verarbeitenden Stelle aus.
Es gelten folgende erweiterten Sicherheitsstandards:

6.1 Alle internen und externen Mitarbeiter werden regelmäßig über Maßnahmen zur Informationssicherheit geschult und sind verpflichtet, diese einzuhalten.

Mitarbeiter spielen in der Mehrheit der IT-Sicherheitsvorfälle eine entscheidende Rolle. Wenn technische Schutzmaßnahmen einen Angriff effektiv verhindern, werden Angreifer versuchen, ihr Angriffsziel auf anderem Weg zu erreichen und bedienen sich dabei nicht selten Mitteln der Täuschung. Mitarbeiter sollten daher regelmäßig im Erkennen solcher Angriffsversuche geschult werden.

Zudem müssen speziell im Umgang mit sensiblen Personendaten alle Mitarbeiter ausreichend zur Informationssicherheit geschult sein. Eine Möglichkeit bieten hierfür sogenannte Awareness-Trainings. Über rechtliche Änderungen zum Umgang mit personenbezogenen Daten muss der Mitarbeiter zeitnah informiert werden. Eine regelmäßige Auffrischung sollte hierbei alle 1 bis 3 Jahre stattfinden. Neu hinzukommende Mitarbeiter sind grundsätzlich über die Daten- und Informationssicherheit zu schulen.

6.2 Beim Ausscheiden von Mitarbeitern werden deren Zugänge unverzüglich gesperrt.

Systemzugänge und Kennwörter dürfen nach dem Ausscheiden des Mitarbeiters aus dem Unternehmen (Ende des Beschäftigungszeitraums) nicht mehr zur Verfügung stehen. Auch Zugangskarten sowie überlassene Geräte (Laptop, Mobiltelefon etc.) sind vom ehemaligen Mitarbeiter zurückzuverlangen.

6.3 Der Zugriff auf unsere interne IT-Infrastruktur über öffentliche oder drahtlose Netze erfolgt ausschließlich verschlüsselt.

Insbesondere die in Hotels und Konferenzzentren üblichen kabellosen Zugänge stellen oft eine unverschlüsselte drahtlose Verbindung zum Netz dar und können von lokalen Angreifern passiv mitgeschnitten oder aktiv manipuliert werden. Der Zugriff auf kritische Systeme darf daher nur über verschlüsselte und authentifizierte Kanäle erfolgen.
Dies kann z. B. mittels eines VPN (Virtuelles privates Netzwerk) erreicht werden.

6.4 Sensible Daten werden entsprechend ihrem Schutzbedarf beim Speichern, bei der Weitergabe und dem Versenden geschützt (z. B. Verschlüsselung) bzw. mobile Speichermedien werden verschlüsselt.

Mobile Geräte oder Datenträger können im Fall eines Diebstahls oder Verlusts in fremde Hände geraten. Ein einfacher Passwortschutz reicht dann nicht mehr aus, um Angreifer am Auslesen der darauf gespeicherten Daten zu hindern. Eine Vollverschlüsselung aller mobilen Datenträger ist daher erforderlich. Weitere Schutzmaßnahmen können je nach Einsatzzweck eine
– Ortung oder Fernlöschung des Geräts,
– eine Zwei-Faktor-Authentifizierung bei der Nutzung kritischer Ressourcen oder Zugänge und
– andere Maßnahmen sein, die einen Angreifer am Auslesen von Daten oder dem Zugriff auf kritische Ressourcen hindern.

6.5 Es gibt einen Verantwortlichen für die IT-Sicherheit und für die Einhaltung datenschutzrechtlicher Vorgaben.

IT-Systeme und deren Zusammenspiel in einer größeren Organisation erfordern ein Management mit definierten Verantwortlichkeiten.

Seit Einführung der Datenschutz-Grundverordnung bestehen erheblich strengere Anforderungen zum Datenschutz. Um diese Regelungen in geeigneter Form und geeignetem Umfang umsetzen zu können, ist hierzu ein Datenschutzbeauftragter zu bestellen. Für Unternehmen, welche aus datenschutzrechtlicher Sicht einer besonderen Kontrolle bedürfen, besteht sogar die Pflicht.

6.6 Mitarbeiter haben nur die Zugänge und Rechte, welche für die Erfüllung der Tätigkeiten erforderlich sind. Weitergehende Rechte
- **sind ausschließlich Administratoren und zur Erledigung administrativer Tätigkeiten vorbehalten,**
- **werden regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft.**

Es ist nicht nur wichtig, einzelne Benutzer durch individuelle Kennungen zu unterscheiden, sondern diesen Benutzern auch ihrer Tätigkeit entsprechende Rechte zu erteilen. Seit Vista unterscheidet auch Windows unterschiedliche Benutzerebenen (Benutzerkontensteuerung). Admin-Rechte, also ein Vollzugriff auf alle Systeme und Anwendungen, sollten daher den IT-Verantwortlichen vorbehalten sein.
Bei Wechsel im Unternehmen oder bei temporärer Gewährung von erweiterten Zugangsrechten sind die Rechte regelmäßig dem Bedarf anzupassen.

6.7 Die Installation von Sicherheits-Patches für unsere IT wird zentral gesteuert.
Mit der Veröffentlichung von Sicherheitsupdates werden auch die zugrunde liegenden Software-Schwachstellen der allgemeinen Öffentlichkeit bekannt. Dadurch steigt das Risiko des Betriebs nicht aktueller Software.

6.8 Es bestehen technische Mindestanforderungen an die Zugangspasswörter (min. 8 Zeichen; Zahlen und Buchstaben; Groß- und Kleinschreibung).
Kennwörter müssen in einem regelmäßigen Turnus geändert werden.
Es gibt Computerprogramme, die mit der Brute-Force-Methode* versuchen, ein Passwort zu erraten. Ausgehend von Buchstaben, Zahlen und Sonderzeichen würden heutige Rechner bei vier Zeichen weniger als eine Sekunde benötigen. Bei sieben Zeichen dauert es 21 Stunden. Ab dem achten Zeichen sind es schon 84 Tage. Das neunte Zeichen verlängert die Dauer auf 22 Jahre.

*Bei einem Brute-Force-Angriff werden durch einen leistungsstarken PC automatisiert alle möglichen Zeichenkombinationen für ein Passwort ausprobiert. Heutzutage prüft ein durchschnittlicher PC gut mehrere Millionen Passwörter pro Sekunde. Sie sollten deshalb immer eine Kombination aus Buchstaben, Sonderzeichen und Ziffern für Ihr Passwort verwenden sowie auf eine angemessene Länge achten.

Neben der Verwendung eines starken Passworts gilt es allerdings noch mehr zu beachten: So sollten Sie kein Passwort mehrfach verwenden. Denn ist erst einmal eine Anwendung oder ein Dienst kompromittiert, was leider immer wieder vorkommen kann, dann wären damit auch Ihre anderen Accounts mit demselben Passwort gefährdet.
Zudem muss ein Kennwort auch regelmäßig, mindestens im Jahresturnus, geändert werden.

Über diese Sicherheitshinweise informiert auch das Bundesministerium des Inneren:
https://www.sicher-im-netz.de/sicheres-passwort

6.9 Es sind Vorkehrungen für einen IT-Notfall (Wiederanlaufkonzept) getroffen und Verantwortliche benannt.
Ein Notfallwiederherstellungsplan (oder im Englischen Disaster Recovery) stellt systematisch alle Maßnahmen dar, welche nach einem Störfall getroffen werden müssen und wer dafür verantwortlich ist.
Hierzu zählt u. a. die Identifizierung kritischer Unternehmensinfrastruktur, -organisation und Hardware sowie deren Wiederherstellung bzw. Ersatz.

Häufig stellt ein Wiederanlaufkonzept einen Teil der Business Continuity dar, welches unterbrechungsfreie Geschäftsabläufe sicherstellen soll.

7003001153-201803

HDI Versicherung AG
HDI-Platz 1
30659 Hannover
www.hdi.de/cyberversicherung