HDI Versicherung AG
www.hdi.de

Risikoanalyse zur Cyberversicherung für tarifliche Risiken für Firmen und Freie Berufe mit Jahresumsatz bis 10 Mio. EUR inkl. Erläuterungen

Unternehmen mit Jahresumsätzen größer 10 Mio. EUR, produzierendes Gewerbe mit automatisierten Produktionsprozessen (ICS) und Unternehmen im Gebiet der Infromationstechnologie verwenden den HDI Cyber Risiko Checkup.

Partner-Nr. _____

Betreuer-Nr. _____

Vermittler-Nr./VP _____

Interessent

☐ Frau ☐ Herr ☐ Firmierung Name/Vorname/Firmierung

_____

_____

Straße/Nr. _____

PLZ/Ort _____

Telefon _____

Mobil _____

Telefax _____

E-Mail _____

Internet _____

Zielgruppe _____ WZ-Code _____

Erstniederlassung bzw. Gründungsdatum _____

Büro Anschriften _____

_____

Ohne ausdrückliche Benennung sind als rechtlich selbständige Tochtergesellschaften existierende Gesellschaften innerhalb der Bundesrepublik Deutschland mitversichert, sofern keine abweichende Tätigkeit vorliegt.

Ist die Mitversicherung weiterer rechtlich selbstständiger Unternehmen gewünscht? ☐ ja ☐ nein

Bitte geben Sie den/die Namen und Anschrift/en an. Falls der Platz hier nicht ausreicht, fügen Sie bitte ein separates Blatt an.

Name _____ PLZ/Ort _____

Straße/Nr. _____

Umfassen die Antworten in diesem Fragebogen alle (mit)versicherten Unternehmen des Versicherungsnehmers? ☐ ja ☐ nein

(Wenn nein, bitte für diese Unternehmen eine eigene Risikoanalyse einreichen)

Tätigkeitsbeschreibung

Branchengruppe _____

Jahresumsatz _____ EUR

davon aus Onlinegeschäften _____ EUR

Bei einem Umsatz größer 10.000.000 EUR reichen Sie bitte den HDI Cyber Risiko Checkup ein.

Tätigkeitsbeschreibung _____

gewünschter Deckungsumfang

Versicherungssumme in EURO ☐ 100.000 ☐ 250.000 ☐ 500.000 ☐ 750.000 ☐ 1 Mio. ☐ 2 Mio. ☐ _____

Selbstbeteiligung je Schadenfall in EURO ☐ 500 ☐ 1.000 ☐ 2.500 ☐ 5.000 ☐ _____

Wartezeit bei Betriebsunterbrechung ☐ 12 Stunden ☐ _____

Optionale Bausteine

☐ **Cyber Betriebsunterbrechung durch Cloudausfall**
Betriebsunterbrechung durch den Ausfall einer beruflich und entgeldlich genutzten Cloud

☐ **Cyber Betriebsunterbrechung durch technische Störung**
Cyber Betriebsunterbrechung in Folge einer technischen Störung durch, z.B. Über- und Unterspannung, Überhitzung oder unterlassenes IT-Systemupgrade

☐ **Cyber Security Baustein:**
Jährlicher Check der IT-Systeme zur Ermittlung des aktuellen Sicherheitsniveaus und Erhalt von Verbesserungspotenzialen

7003001127-202410

Risikofragen

1. Besitzen alle Nutzer individuelle, passwortgeschützte Zugänge und unterscheidet das betriebene IT-System in unterschiedliche Befugnisebenen? ☐ ja ☐ nein
2. Setzen Sie einen Schutz gegen Schadsoftware (z.B. Antivirensoftware) ein, der automatisch auf dem aktuellen Stand gehalten wird? ☐ ja ☐ nein
3. Sind Ihre IT-Systeme mit einem zusätzlichen Schutz gegen unberechtigten Zugriff (z.B. Firewall) ausgerüstet, wenn diese über das Internet (z.B. Server) erreichbar sind oder es sich um Mobilgeräte handelt? ☐ ja ☐ nein
4. Werden im Rahmen eines Patch-Management-Verfahrens vom Hersteller bereitgestellte Sicherheitsupdates zeitnah eingespielt? ☐ ja ☐ nein
5. Nicht mehr unterstützte Software (End-of-Life) wird nicht betrieben? ☐ ja ☐ nein
6. Unterliegen die IT-Systeme einem wöchentlichen Sicherungsprozess, wobei die Sicherungsdatenträger physisch getrennt und vor dem Zugriff Unberechtigter gesichert aufbewahrt werden? ☐ ja ☐ nein
7. Wird regelmäßig (mind. jährlich) geprüft, dass eine Rücksicherung bei Bedarf einwandfrei durchgeführt werden kann? ☐ ja ☐ nein
8. Haben Sie alle vom Hersteller voreingestellten Passwörter auf allen Geräten in Ihrem Netzwerk (z.B. Telefonanlagen, Anrufbeantwortern, Drucker, Router, IoT-Geräte) geändert? ☐ ja ☐ nein
9. Erfolgt der Zugriff auf die interne IT-Infrastruktur über öffentliche oder drahtlose Netze ausschließlich verschlüsselt? ☐ ja ☐ nein

Zusatzfragen für Unternehmen aus den Bereichen Unternehmensberatung / Ingenieurwesen / Werbeagentur / Beratungsleistungen auf dem Gebiet der Informationssicherheit

10. Es wird KEINE Softwareentwicklung für Dritte betrieben?? ☐ ja ☐ nein
11. Sie bieten KEINE "as a Service" Dienstleistungen an oder Sie hosten KEINE Dienste für Dritte? ☐ ja ☐ nein

Sollten Sie eine der Fragen mit "nein" beantwortet haben, bitten wir Sie in der Anlage hierzu nähere Angaben zu machen. Vielen Dank.

Vorversicherung

☐ keine Vorversicherung ☐ bei HDI, Versicherungs-Nr. _____

☐ anderweitig, Name des Versicherers und VS-Nr.: _____

Aus den letzten 5 Jahren sind keine Schäden durch eine Daten- oder Cyberrechtsverletzung, Hacker-Angriff, Denial-of-Service- Angriff oder Cyber-Erpressung bekannt und Ihnen sind auch keine Umstände bekannt, die zu einem Cyber-Versicherungsfall führen könnten. ☐ ja ☐ nein

Anzahl der Schäden und Aufwendungen _____

Keine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen den Versicherungsnehmer oder eine mitversicherte Person eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht. ☐ ja ☐ nein

Geben Sie auch alle Fälle an, die ohne eine Zahlung (zu Ihren Gunsten) geschlossen wurden.
Bitte beachten Sie: Bei einer Falschangabe ist der Versicherer zum Rücktritt wegen vorvertraglicher Anzeigepflichtverletzung berechtigt.

Ablauf der Vorversicherung _____

☐ Kündigung durch Versicherungsnehmer ☐ Kündigung durch Versicherer

Prämienzahlung/ Vertragslaufzeit

Versicherungsbeginn: _____ 0 Uhr Versicherungsablauf: _____ 0 Uhr Nächste Prämienfälligkeit: _____

Prämie zahlbar: ☐ jährlich ☐ 1/2-jährlich (3 % Zuschlag)

Wichtiger Hinweis

Bitte beachten Sie, dass der Versicherer seine Entscheidung über die Annahme des Antrags auf die wahrheitsgemäße Erklärung stützt. Unwahre oder unvollständige Angaben können den Versicherer zum Rücktritt vom Vertrag berechtigen, unter Umständen sogar zur Anfechtung wegen arglistiger Täuschung, die den Versicherungsschutz rückwirkend (von Anfang an) entfallen lässt.

Ort/Datum _____ Unterschrift X _____

Nähere Angaben zu den Risikofragen

Zu Frage _____ _____

Zu Frage _____ _____

Zu Frage _____ _____

Zu Frage _____ _____

Erläuterungen zu den Risikofragen

Besitzen alle Nutzer individuelle, passwortgeschützte Zugänge und unterscheidet das betriebene IT-System in unterschiedliche Befugnisebenen?

Jeder Mitarbeiter sollte nur die für die eigene Tätigkeit notwendigen Berechtigungen und Zugänge erhalten. Somit kann unbefugtem Zugriff und Missbrauch von Rechten vorgebeugt werden. Lokale Administratorrechte sollten nur Administratoren besitzen, die diese weitreichenden Berechtigungen für die tägliche Arbeit benötigen. Diese stellen nicht nur eine Gefahr hinsichtlich unbeabsichtigter oder böswilliger Aktivitäten der Endnutzer (z.B. Installation von Schadsoftware, Konfiguration der Firewall) dar, sondern sind auch für Angreifer ausnutzbar. Wurde ein Account mit lokalen Administratorrechten kompromittiert, kann sich der Angreifer weitere Zugangsdaten beschaffen, Sicherheitsvorkehrungen deaktivieren und sich durch das Firmennetz bewegen, um z.B. Zugriff zu weiteren privilegierten Benutzerkonten zu erlangen. Somit kann der Angreifer im schlimmsten Fall Zugriff auf die gesamte IT-Infrastruktur bekommen und diese ausnutzen.
Außerdem sollte jeder Mitarbeiter einen eigenen Account besitzen, der mit den für die Tätigkeit notwendigen Berechtigungen ausgestattet ist. Besitzen Mitarbeiter weitreichende Berechtigungen, kann nie vollständig ausgeschlossen, dass diese beabsichtigt oder unbeabsichtigt missbraucht werden. Das Teilen von Accounts (sog. Shared User Accounts) sollte unterbunden werden und birgt zahlreiche Risiken. Laut Art. 32 DSGVO müssen Benutzer bei Anmeldungen an Datenverarbeitungssystemen eindeutig identifiziert und authentisiert werden, um eine ausreichende Vertraulichkeit und Integrität der Daten zu gewährleisten. Wird dies nicht umgesetzt, besteht zum einen das Problem, dass die Zugriffsrechte der einzelnen Benutzer, je nach Aufgabenstellung oder Tätigkeitwechsel, innerhalb des Systems nicht differenziert vergeben werden können. Außerdem kann nicht nachvollzogen werden, wer wann auf welche Daten zugegriffen hat bzw. diese bearbeitet oder verändert hat. Wurde im Namen des geteilten Accounts eine für das Unternehmen ungewollte oder schädliche Handlung ausgeführt, kann nicht nachgewiesen werden, wer den festgestellten Missbrauch begangen hat. Auch Angreifer und Unbefugte nutzen diese Anonymität dieser Accounts gerne aus, um dem Unternehmen zu schaden. Weiterhin ist die Vertraulichkeit der Passwörter bei Shared User Accounts nicht gewährleistet. Bei einem Passwortwechsel muss das neue Passwort mehreren Mitarbeitern mitgeteilt werden. Dabei besteht die Gefahr, dass das Passwort durch Dritte ausgespäht wird. Außerdem müssen sich mehrere Leute das gleiche Passwort merken, weshalb oftmals einfache Passwörter gewählt werden.

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 unkritischer 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).

Mittlerweile existieren zahlreiche Methoden, um Passwörter durch wahlloses Ausprobieren von Zeichenkombinationen herauszufinden. Bei so genannten „Brute-Force-Angriffe" probieren leistungsstarke Computer automatisiert alle möglichen Zeichenkombinationen für ein Passwort aus. Weiterhin gibt es Angriffe, bei denen mit Hilfe von Passwortlisten versucht wird, ein unbekanntes Passwort zu ermitteln. Daher sollten auf einfache Wörter oder Namen verzichtet werden. Die zwei genannten Methoden zeigen, wie professionell heutzutage Angreifer vorgehen. Umso wichtiger wird die Verwendung eines komplexen Passworts. Allgemein gilt, dass die Verwendung eines komplexen, langen Passworts einen effektiveren Schutz liefert als die Verwendung eines weniger komplexen Passworts, das regelmäßig geändert wird. Neben der Verwendung eines komplexen Passworts, sollte kein Passwort mehrfach verwendet werden. Wurde eine Anwendung oder ein Dienst kompromittiert, werden die hinterlegten Accounts oftmals veröffentlicht oder verkauft, wodurch sämtliche Accounts in Gefahr sind, bei denen Sie dasselbe Passwort verwendet haben.

Gemäß BSI sollten Passwörter (derzeit) folgenden Kriterien entsprechen:

- Länge: Mindestens acht Zeichen haben
- Verwendung von Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen
- Vermeidung von Passwörtern aus gängigen Passwortlisten oder dem Wörterbuch
- Vermeidung der Wiederverwendung der letzten Passwörter
- Keine Mehrfachverwendung von Passwörtern (für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden)
- Passwörter müssen gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht
- Passwörter müssen so sicher wie möglich gespeichert werden

Setzen Sie einen Schutz gegen Schadsoftware (z.B. Antivirensoftware) ein, der automatisch auf dem aktuellen Stand gehalten wird?

Schutz gegen Schadsoftware (Malware) kann zum Beispiel in Form eines Antivirenprogramms umgesetzt werden. Dabei ist es enorm wichtig, dass das Programm stets auf dem aktuellen Stand gehalten wird, da sich die Angriffslage ständig verändert und neue Schadsoftware entwickelt wird. Dieser Schutz sollte auf sämtlichen vom Versicherten betriebenen Hard- und Softwaresystemen sowie Endgeräten eingesetzt und aktiviert werden. Eine automatische Aktualisierung sollte sichergestellt sein. Auch hier gilt, dass vom Hersteller nicht mehr unterstützte Software zeitnah auf den aktuellen Stand umgestellt werden sollte.

Möglichkeiten sind handelsübliche Antivirenprogramme oder auch die betriebssystemeigene Schutzsoftware (z.B. Windows Defender).

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.

Sind Ihre IT-Systeme mit einem zusätzlichen Schutz gegen unberechtigten Zugriff (z.B. Firewall) ausgerüstet, wenn diese über das Internet (z.B. Server) erreichbar sind oder es sich um Mobilgeräte handelt?

Insbesondere IT-Systeme die über das Internet erreichbar sind (z.B. Server) oder Mobilgeräte umfassen, sollten mit einem zusätzlichen Schutz gegen unberechtigten Zugriff ausgestattet sein. Dies kann in Form einer Firewall erreicht werden. Die Bedeutung einer Firewall liegt darin, den Datenverkehr zwischen IT-System und Internet zu überwachen und zu kontrollieren. Durch diese Überwachung kann die Firewall unautorisierte Zugriffsversuche erkennen und blockieren. Dies ist von entscheidender Bedeutung, da das Internet eine Vielzahl von potenziellen Bedrohungen wie Hackerangriffe, Viren oder andere Malware birgt. Dies trägt dazu bei, die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten und potenzielle Sicherheitslücken zu schließen.

Nicht nur der Server sollte geschützt werden. Eine Personal- / Desktop-Firewall sollte auf allen mit dem Internet verbundenen Geräten installiert, aktiviert und aktualisiert sein. Je nach Unternehmensgröße kann die vorinstallierte Firewall von gängigen Betriebssystemen (Windows, MacOS) ausreichend sein.

Werden im Rahmen eines Patch-Management-Verfahrens vom Hersteller bereitgestellte Sicherheitsupdates zeitnah eingespielt?

Patches werden veröffentlicht, um ein oder mehrere Probleme (z.B. Schließen von Sicherheitslücken) einer Software zu beheben. Beinhalten Patches neue Funktionen der Software, wird von einem Update gesprochen.
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 (z.B. Adobe Reader, Internetbrowser und MS Office) zu legen.
Durch den Hersteller bereitgestellte Patches und Updates sollten zeitnah nach Veröffentlichung (ohne schuldhafte Verzögerung) eingespielt werden. Nicht mehr unterstützte Software muss zeitnah auf einen aktuellen Stand umgestellt werden.
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.

Nicht mehr unterstützte Software (End-of-Life) wird nicht betrieben?

Nicht mehr unterstützte Software stellt ein erhebliches Sicherheitsrisiko dar. Wenn eine Software keine regelmäßigen Updates und Sicherheitspatches mehr erhält, bleiben mögliche Schwachstellen und Sicherheitslücken ungeschlossen. Dies macht es für potenzielle Angreifer einfacher, auf das IT-System zuzugreifen und Daten zu kompromittieren oder Schaden anzurichten.

Daher sollte keine Software betrieben werden, die nicht mehr unterstützt wird oder deren End-of-Life erreicht wurde. Stattdessen sollte auf aktuelle und unterstützte Softwarelösungen, die Updates und Sicherheitspatches erhalten, umgestiegen werden. Dadurch wird sichergestellt, dass das IT-System mit den neuesten Sicherheitsstandards kompatibel ist und mögliche Sicherheitsrisiken minimiert werden.

Aktuelle, vom Hersteller unterstützte Software trägt zur Sicherheit und Stabilität des IT-Systems bei und schütz die Daten vor potenziellen Bedrohungen.

Unterliegen die IT-Systeme einem wöchentlichen Sicherungsprozess, wobei die Sicherungsdatenträger physisch getrennt und vor dem Zugriff Unberechtigter gesichert aufbewahrt werden?

Ohne Datensicherung (Backup) ist eine Wiederherstellung der Betriebsbereitschaft kaum möglich. Ein nachhaltiger Datenverlust bedeutet darüber hinaus nicht selten eine lang andauernde Betriebsunterbrechung. Es sollte mindestens eine wöchentliche Sicherung aller Daten (Vollsicherung) stattfinden. Idealerweise werden geschäftskritische / sensible Daten täglich gesichert.
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.

Backups sollten außerdem vor Manipulation oder unbefugtem Zugriff geschützt werden. Wenn Backups nachträglich vom betroffenen System oder vom Angreifer verändert werden können, besteht das Risiko, dass sie ebenfalls zu Schaden kommen.
Hinweis: Da eine NAS-Speicherlösung (Network-attached Storage) eine physische Netzwerkverbindung erfordert ist es möglich, dass auch der NAS-Speicher bei einem Angriff befallen sein kann und somit das Backup unbrauchbar ist. Anders ist dies bei cloudbasierten Lösungen. Diese können durch Ihre physische Trennung vom IT-System zuverlässigen Schutz des Backups bei einem Angriff bieten, wenn Sie mit einem zusätzlichen Schutz vor unberechtigtem Zugriff abgesichert sind.

Wird regelmäßig geprüft (mind. Jährlich), dass eine Rücksicherung bei Bedarf einwandfrei durchgeführt werden kann?

Eine regelmäßige Überprüfung der Wiederherstellung durch das Backup stellt sicher, dass diese auch im Ernstfall vollständig funktioniert. Findet eine solche regelmäßige Prüfung nicht statt, sind aufgrund des unerprobten Vorgangs Probleme durch Beschädigung 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.

Haben Sie alle vom Hersteller voreingestellten Passwörter auf allen Geräten in Ihrem Netzwerk (z.B. Telefonanlagen, Anrufbeantwortern, Drucker, Router, IoT-Geräte) geändert?

Standardpasswörter stellen ein erhebliches Sicherheitsrisiko dar und sollten vor der ersten Nutzung geändert werden. Idealerweise wird die Änderung technisch erzwungen. Diese Passwörter folgen einer definierten Logik und können sogar wiederholend vorkommen.

Werden diese nicht geändert, können oftmals gängige Sicherheitsanforderungen für Passwortsicherheit nicht erfüllt werden. Aus diesen Gründen stellen Standardpasswörter eine enorme Schwachstelle dar und sind ein beliebtes Ziel für Angreifer. Durch die Vernetzung der Geräte (z.B. Drucker, Router) bieten sie ein beliebtes Einfallstor für Angreifer, die auf diesem Weg oftmals auch auf weitere Teile des Netzwerks zugreifen.

Erfolgt der Zugriff auf die interne IT-Infrastruktur über öffentliche oder drahtlose Netze ausschließlich verschlüsselt?

Öffentliche WLAN-Netzwerke, z.B. in Hotels, Konferenzzentren oder Restaurants, stellen oft eine unverschlüsselte drahtlose Verbindung zwischen dem mobilen Gerät und dem Router dar und können von lokalen Angreifern passiv mitgeschnitten oder aktiv manipuliert werden. Nach Beendigung der Verbindung sollte das Netzwerk außerdem aus der Liste der gespeicherten WLAN-Netzwerke gelöscht werden, um ein unbewusstes, automatisches Einwählen zu verhindern. Der Zugriff auf kritische Systeme oder der Austausch von vertraulichen Daten darf daher nur über verschlüsselte und authentifizierte Kanäle erfolgen. Dies kann z.B. mittels eines VPN (Virtuelles privates Netzwerk) erreicht werden. Ein VPN ist ein sicherer Tunnel zwischen zwei oder mehreren Geräten und bietet die Möglichkeit von außen (z.B. mit einem Laptop) auf ein bestehendes Netzwerk (z.B. Unternehmensnetzwerk) zuzugreifen. Mit Hilfe eines VPNs kann sichergestellt werden, dass die Kommunikation zum bestehenden Netzwerk nicht mitgelesen wird. Außerdem besteht so die Möglichkeit von außen auf unternehmensinterne Laufwerke zuzugreifen.

Es wird KEINE Softwareentwicklung für Dritte betrieben?

Hierunter fällt die Entwicklung von Software deren Nutzung für andere Unternehmen oder Personen bestimmt ist. Dies können u.a. benutzerdefinierte Softwarelösungen, Anwendungen oder Websites sein.

Sie bieten KEINE "as a Service" Dienstleistungen an oder Sie hosten KEINE Dienste für Dritte

"As a Service" bedeutet, dass Dienstleistungen über das Internet bereitgestellt werden, normalerweise gegen eine Abonnementgebühr. Viele Unternehmen bieten Dienste und Hosting-Services für andere Unternehmen oder Personen an. Beispiele dafür sind Software as a Service (SaaS), bei dem Softwareanwendungen über das Internet bereitgestellt und genutzt werden können, Infrastructure as a Service (IaaS), bei dem Unternehmen Zugriff auf technische Infrastruktur wie Server, Speicherplatz und Netzwerkressourcen erhalten, oder Platform as a Service (PaaS), bei dem eine Entwicklungsplattform über das Internet bereitgestellt wird, um Anwendungen zu entwickeln und bereitzustellen. Durch das Hosten von Diensten für Dritte stellt ein Unternehmen seine technische Infrastruktur zur Verfügung, damit andere Unternehmen oder Personen Anwendungen oder Websites auf ihren Servern betreiben können.