

Häufig gestellte Fragen (FAQ): Risikomanagement für die Microsoft Online Services (Standard-Version)

Letzte Aktualisierung: 16. September 2009

Inhaltsverzeichnis

Sicherheit.....	2
Compliance.....	4
Datenschutz.....	9
Dienstkontinuität.....	10

Die in diesem Dokument enthaltenen Informationen stellen die zum Veröffentlichungszeitpunkt aktuelle Ansicht der Microsoft Corporation zu den darin besprochenen Themen dar. Da Microsoft auf sich ändernde Marktbedingungen reagieren muss, sollten sie nicht als eine Verpflichtung seitens Microsoft interpretiert werden, und Microsoft kann die Genauigkeit der Informationen nach dem Veröffentlichungsdatum nicht garantieren.

Diese Dokument dient ausschließlich Informationszwecken. MICROSOFT BIETET KEINE AUSDRÜCKLICHEN, IMPLIZITEN ODER LEGALEN GARANTIE BEZÜGLICH DER IN DIESEM DOKUMENT WIEDERGEgebenEN INFORMATIONEN.

Die Einhaltung aller zutreffenden Copyright-Gesetze liegt in der Verantwortung des Benutzers. Ohne dass hierdurch die Copyright-Rechte eingeschränkt würden, darf kein Teil dieses Dokuments zu irgendeinem Zweck ohne die ausdrückliche schriftliche Genehmigung der Microsoft Corporation reproduziert, in ein Speichersystem eingegeben oder in diesem gespeichert oder in irgendeiner Weise oder in irgendeiner Form übertragen werden (elektronisch, mechanisch, durch Fotokopieren, Aufnahmen oder auf sonstige Art und Weise).

Microsoft verfügt möglicherweise über Patente, Patentanmeldungen, Warenzeichen, Copyright oder andere geistige Eigentumsrechte bezüglich der in diesem Dokument besprochenen Themen. Indem Ihnen dieses Dokument zur Verfügung gestellt wird, wird Ihnen keine Lizenz für diese Patente, Warenzeichen, Copyright-rechte oder anderes geistiges Eigentum erteilt, es sei denn, dies ist ausdrücklich in einer schriftlichen Lizenzvereinbarung mit Microsoft vereinbart.

© (2009) Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft Exchange, Microsoft Forefront und Microsoft SharePoint sind entweder eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern.

Die Namen von hierin erwähnten tatsächlichen Unternehmen und Produkten können Warenzeichen ihrer jeweiligen Eigentümer sein.

Sicherheit

Frage: Woher wissen Kunden, dass ihre Informationen bei Microsoft Online Services sicher aufgehoben sind?

Unternehmen müssen eine Kombination von Technologien und Prozessen benutzen, um ihre Systeme für Kommunikation und Zusammenarbeit vor internen und externen Sicherheitsbedrohungen zu schützen. Solche Bedrohungen beruhen auf einer Vielzahl möglicher Angriffswege, deren Abwehr die Einrichtung multipler Schutzebenen erfordert. Kunden können ihre eigenen Sicherheitskontrollen und -prozesse mit Microsoft Online Services erweitern, indem sie:

- Risiken durch ein umfassendes Programm verwalten, das Sicherheit, Datenschutz, Dienstkontinuität und Compliance-Management beinhaltet.
- Mehrfache Ebenen von physischen und logischen Sicherheitskontrollen sowie mehrere Technologien einsetzen.
- Riskomanagementkontrollen und -vorgehensweisen an anerkannten Standards wie ISO 27001 und SAS 70 ausrichten und diese Kontrollen und Vorgehensweisen regelmäßig anhand von Zertifizierungen durch Drittanbieter bestätigen lassen.

FRAGE: Wie viele Microsoft-Mitarbeiter verfügen über Administratorrechte? Mit anderen Worten, wie viele Personen verfügen über möglichen Zugang zu Daten?

Die Anzahl von Microsoft-Mitarbeitern mit Administratorzugang variiert je nach Dienst. Der Zugriff auf Microsoft Online Services-Umgebungen für den Dienstleistungssupport und Administratoren ist durch starke Authentifizierungsvorgänge geschützt, die innerhalb jedes Dienstes physische und logische Isolierung fordern. Innerhalb von Microsoft Online Services wird jedem Mitarbeiter ein individuelles Benutzerkonto für Wartungsaktivitäten zur Verfügung gestellt. Der Zugang zur Microsoft Online Services-Umgebung wird in Abhängigkeit von der Funktion der jeweiligen Person und ihrer geschäftlichen Anforderungen gewährt. Die Benutzerkonten erhalten Benutzerprivilegien auf der Grundlage von „Least Privilege“- und „Need-to-Know“-Prinzipien. Benutzerkonten werden geschlossen, sobald sich der Anstellungsstatus eines Mitarbeiters ändert. Die Benutzerkonten werden periodisch abgeglichen, um sicherzustellen, dass jeder gewährte Zugang notwendig ist und weiterhin mit der Funktion der Person übereinstimmt.

FRAGE: Wie verhindert Microsoft, dass Administratoren auf Kundendaten zugreifen können?

Obwohl Datenbankadministratoren definitionsgemäß auf alle Ressourcen einer Datenbank zugreifen können, inklusive der Kundendaten, untersagt Microsoft den Zugriff auf Kundendaten für Zwecke, die nicht durch geschäftliche Erfordernisse gegeben sind. Erlaubt wäre demnach z.B. der Zugriff, um die Leistung von Datenbanken zu steigern, Kunden von einer Datenbank auf eine andere zu migrieren, Dienste und andere für die Leistungserstellung benutzte Microsoft-Produkte und -Dienste zu verbessern oder um auf rechtliche Anfragen zu antworten.

Alle Microsoft-Mitarbeiter sind für den Umgang mit Kundendaten rechenschaftspflichtig: Der Zugang zu Microsoft Online Services wird in einer Weise gewährt, die ihn jeweils auf einen einzigen Benutzer zurückverfolgen lässt. Mit anderen Worten wird die Rechenschaftspflicht durch ein Bündel von

Systemkontrollen durchgesetzt, darunter die Benutzung von einmaligen Benutzernamen, Datenzugangskontrollen und Prüfverfahren. Anders als bei generischen Benutzernamen wie „Gast“ oder „Administrator“ werden eindeutige Benutzernamen verwendet, um die Rechenschaftspflicht durchzusetzen, indem Benutzerhandlungen jeweils mit einer spezifischen Person verknüpft werden. Ferner wird Zweifaktorauthentifizierung, wie z.B. Smartcard-Anmeldungen mit digitalen Zertifikaten oder RSA-Tokens, benutzt, um diese Verknüpfung zu verstärken.

Der Benutzerzugriff auf Daten wird auch durch die Funktion des jeweiligen Benutzers eingeschränkt. So erhalten z.B. Systemadministratoren keinen Administratorzugang zu Datenbanken.

Microsoft wendet strenge Kontrollen darauf an, welche Benutzerrollen und welche Benutzer Zugang zu Kundendaten erhalten. So werden z.B. aktuell alle Microsoft-Mitarbeiter in den USA vor der Einstellung einer Sicherheitsprüfung unterzogen. Benutzer müssen ein Formular ausfüllen und begründen, warum sie aus geschäftlichen Gründen Zugang benötigen. Bevor der Zugang gewährt wird, muss der Manager des Benutzers seine Genehmigung erteilen. Ferner werden die Zugangsberechtigungen regelmäßig überprüft, um sicherzustellen, dass nur diejenigen Benutzer Zugang zu den Systemen erhalten, die ihn benötigen. Wenn Microsoft-Mitarbeiter das Unternehmen verlassen, durchlaufen sie ein Verfahren, bei dem ihr logischer und physischer Zugang aufgehoben wird.

Außerdem verfügen die Rechenzentren, auf denen Microsoft Online Services gehostet werden, über biometrische Zugangskontrollen. Bei den meisten sind Handabdrücke für den physischen Zugang erforderlich. Weitere Informationen zu den auf Microsoft Online Services gespeicherten Kundendaten stehen in der [Microsoft Online Services-Datenschutzbestimmungen](#)-Erklärung, den [Microsoft's Privacy Guidelines For Developing Software Products and Services](#) und dem [Whitepaper „Sicherheitsfeatures in Microsoft Online“](#) zur Verfügung.

FRAGE: Wie identifiziert, stoppt und korrigiert Microsoft unberechtigte Datenzugriffe und wie werden Kunden darüber benachrichtigt?

Microsoft hat stabile Prozesse entwickelt, um eine koordinierte Reaktion auf Sicherheitszwischenfälle zu ermöglichen, darunter Identifizierung, Eingrenzung, Behebung und Wiederherstellung.

Identifizierung - System- und Sicherheitsmeldungen werden erfasst, korreliert und analysiert. Zwischenfälle werden von Betriebs- und Sicherheitsteams von Microsoft Online Services untersucht. Wenn ein Zwischenfall sicherheitsrelevant ist, wird er einer Bedrohungsklasse zugeteilt und innerhalb von Microsoft entsprechend eskaliert. Die Eskalation erfolgt unter Einbeziehung von Produkt-, Sicherheits- und technischen Spezialisten.

Eingrenzung – Das Eskalationsteam beurteilt den Umfang und die Auswirkungen des Zwischenfalls. Die erste Priorität des Eskalationsteams besteht darin, den Zwischenfall einzugrenzen und die Datensicherheit zu gewährleisten. Das Eskalationsteam formuliert die Reaktion, führt entsprechende Tests durch und führt Veränderungen ein. Falls tiefere Untersuchungen erforderlich sind, werden mit branchenweit führender forensischer Software und in bewährter Vorgehensweisen Inhalte von den betroffenen Systemen gesammelt.

Behebung – Nachdem die Situation eingegrenzt wurde, begibt sich das Eskalationsteam daran, etwaige durch den Sicherheitszwischenfall verursachte Schäden zu beheben und die Ursache zu

identifizieren. Falls eine Sicherheitslücke identifiziert wurde, benachrichtigt das Sicherheitsteam die Produktentwicklung.

Wiederherstellung – Während der Wiederherstellung werden Software- oder Konfigurationsaktualisierungen auf das System angewendet und die Dienste werden in ihren kompletten Leistungsumfang zurückversetzt.

FRAGE: Wie hilft Microsoft Kunden, Nachforschungen zu Mitarbeitern des Kunden anzustellen?

Das Microsoft Online Services-Sicherheitsteam darf Kunden operativ bei Sicherheitsfragen unterstützen, die diese anhand der verfügbaren Protokolle und Werkzeuge des Microsoft Online Services-Systems nicht selbst durchführen können. Eine solche Unterstützung wird fallweise durchgeführt, abhängig von der Situation und dem erforderlichen Ressourcenumfang.

FRAGE: Können Kunden auf periodische Berichte zugreifen, in denen die Ergebnisse von Sicherheitsprüfungen, versuchten Angriffen usw. beschrieben werden?

- CyberTrust steht auf der CyberTrust-Website zur Verfügung.
- Microsoft strebt SAS 70 für die Dienste an, die in BPOS Standard enthalten sind, sowie ISO 27001 für BPOS Standard. Berichte werden Kunden zugänglich gemacht, wenn sie verfügbar sind.
- Manche Kunden haben uns wissen lassen, dass sie diese Detailfülle lieber NICHT erhalten würden – dies sei einer der Gründe, warum sie überhaupt erst einen Onlinedienst in Anspruch nehmen. Wir untersuchen dennoch die Möglichkeit, Kunden häufigere, detaillierte Berichte über den Dienststatus, Zwischenfälle usw. zur Verfügung zu stellen.

Compliance

FRAGE: Wo befinden sich die Microsoft Online Services-Rechenzentren? Kann man als Kunde ein bestimmtes Rechenzentrum beanspruchen?

Microsoft verfügt über Rechenzentrums-Standorte verschiedener Größen an unterschiedlichen Standorten weltweit. Microsoft äußert sich öffentlich nicht über die genaue Anzahl oder Standorte seiner Rechenzentren; es gibt jedoch Haupt- und Backup-Rechenzentren, auf denen die Microsoft Online Services angeboten werden, in den folgenden Regionen: Europa, Nordamerika und Asien-Pazifikraum.

FRAGE: Welche Sicherheitsrichtlinien befolgt Microsoft hinsichtlich der Microsoft Online Services?

Die entsprechende Richtlinie „Microsoft Online Services Information Security Policy“ beruht auf ISO 27002-Direktiven, die um Anforderungen speziell für Onlinedienste erweitert wurden. (So verlangt Microsoft zum Beispiel, dass bei jeder größeren Microsoft Online Services-Veröffentlichung Internet-Verwundbarkeitstests durchgeführt werden müssen; falls während solcher Testverfahren kritische Schwachpunkte identifiziert werden, müssen sie vor Freigabe der Dienstversion an Kunden behoben werden.) Die Microsoft Online Services-Informationssicherheitsrichtlinie berücksichtigt auch zusätzliche Anforderungen, die aus klassenführenden Sicherheitsansätzen abgeleitet sind, sowie die Anwendung relevanter internationaler, nationaler und provinzieller (bzw. Landes-) Anforderungen.

ISO 27002 ist Teil der ISO/IEC 27000-Normfamilie, die gemeinsam von der [International Organization for Standardization](#) (ISO) und der [International Electrotechnical Commission](#) (IEC) veröffentlicht wurde und

bei der es sich um die umbenannte, aktualisierte ISO 17799-Norm handelt. Der vollständige Name dieser internationalen Norm lautet *"Information technology - Security techniques - Code of Practice for Information Security Management"*. Die ISO 27000-Norm beansprucht bewusst eine breite Anwendung. Sie deckt Datenschutz, Vertraulichkeit und technische Sicherheitsaspekte ab sowie „bestehende Richtlinien und allgemeine Prinzipien bezüglich der Einleitung, Umsetzung, Pflege und Verbesserung der Informationssicherheitsverwaltung innerhalb einer Organisation“. Die Norm beschreibt zu diesem Zweck Hunderte von potenziellen Kontrollen und Kontrollmechanismen. ISO 27000 wurde unter Berücksichtigung der folgenden Kernprinzipien entwickelt:

„Die Wahrung der Vertraulichkeit (indem sichergestellt wird, dass Informationen nur denjenigen zugänglich gemacht werden, die zum Zugang berechtigt sind), Integrität (indem gewährleistet wird, dass die Informationen und Verarbeitungsmethoden akkurat und vollständig sind) und Verfügbarkeit (indem dafür gesorgt wird, dass berechtigte Benutzer wann immer nötig auf die Informationen und zugehörigen Werte zugreifen können).“¹

Die von ISO 27002 und der Microsoft Online Services Informationssicherheitsrichtlinie berücksichtigten Themenbereiche sind:

- Risikobewertung
- Sicherheitsrichtlinien – Managementvorgaben
- Organisation der Informationssicherheit – Verwaltung der Informationssicherheit
- Asset-Management – Inventarisierung und Klassifizierung des Informationsbestands
- Personalsicherheit – Sicherheitsaspekte bezüglich des Eintritts, der Versetzung oder des Austritts von Mitarbeitern einer Organisation
- Physische und Umweltsicherheit – Schutz der Computereinrichtungen
- Kommunikations- und Betriebsmanagement – Management von technischen Sicherheitskontrollen in Systemen und Netzwerken
- Zugangskontrolle – Einschränkung von Zugangsrechten für Netzwerke, Systeme, Anwendungen, Funktionen und Daten
- Erwerb, Entwicklung und Pflege von Informationssystemen – Integration von Sicherheit in Anwendungen
- Management von Zwischenfällen im Bereich Informationssicherheit – Antizipierung und angemessene Reaktion auf Verletzungen der Informationssicherheit
- Management der geschäftlichen Kontinuität – Schutz, Pflege und Wiederherstellung von geschäftskritischen Prozessen und Systemen
- Compliance – Sicherung der Einhaltung von Informationssicherheitsrichtlinien, Normen, Gesetzen und Vorgaben

FRAGE: Welche Zusicherungen bietet Microsoft hinsichtlich der Sicherheit von Microsoft Online Services?

Die Sicherheit der Microsoft Online Services basiert auf fortschrittlichen Sicherheitsverfahren. Microsoft setzt lückenlose Sicherheitskontrollen (technisch, prozess- und personenbezogen sowie physisch) ein, d.h. von der Produktentwicklung über die Diensteseinführung bis hin zum fortlaufenden Betrieb. Diese Sicherheitskontrollen werden streng durchgesetzt und regelmäßig hinsichtlich ihrer Einhaltung überprüft. Weitere Informationen stehen im [Whitepaper „Sicherheitsfeatures in Microsoft Online“](#) zur Verfügung.

¹ Information Technology—Information security management systems - Requirements, International Standards Organization, ISO/IEC 27001:2005(E)

Die BPOS Standard-Dienste durchlaufen die Cybertrust Security Management Program (SMP)-Perimeterzertifizierung. Das Cybertrust SMP:

- Identifiziert kritische Bestände und die am meisten gefährdeten Bereiche der BPOS Standard-Infrastruktur, wie z.B. mit dem Internet verbundene Systeme.
- Bewertet und priorisiert tatsächliche Bedrohungen für kritische Informationsbestände.
- Hilft, solche Bestände durch effiziente, unternehmensweite Kontroll- und Schadensminimierungsstrategien zu sichern, und
- Sichert die Aufrechterhaltung der Sicherheitsmaßnahmen durch stabilen, fortlaufenden Support.

Der SMP-Zertifizierungsbericht berücksichtigt:

- Eine physische Prüfung aller Rechenzentren vor Ort,
- Interne Schwachstellenanalysen für alle Dienstsegmente,
- Externe Schwachstellenanalysen des Dienstes in allen Rechenzentren,
- Prüfung der Prozesse und Abläufe (mit Systemadministratoren, Netzwerkingenieuren und anderen Schlüsselmitarbeitern, die an der Bereitstellung des Dienstes beteiligt sind) sowie
- E-Mail-Filtertests.

FRAGE: Wer verfügt über Administratorrechte für die Microsoft Online Services-Infrastruktur? Handelt es sich dabei um Vollzeitangestellte oder Vertragsnehmer?

Die Microsoft Online Services werden sowohl von Vollzeitangestellten als auch von Vertragsnehmern betrieben. Es können sowohl Vollzeitangestellte als auch Vertragsnehmer über Administratorrechte für die Microsoft Online Services-Infrastruktur verfügen.

Administratorzugang: Der Zugang zur Microsoft Online Services-Infrastruktur für Administratoren und Benutzer ist beschränkt und wird nur auf der Basis des „need-to-know“-Prinzips zugelassen. Nur operative Mitarbeiter, die für die Verwaltung der Microsoft Online Services-Infrastruktur verantwortlich sind, erhalten Administratorzugang.

Zugang zu Kundendaten: Nur Datenbankadministratoren und Kundensupportmitarbeiter verfügen über Zugang zu Kundendaten. Obwohl Datenbankadministratoren und Supportmitarbeiter auf Kundendaten zugreifen können, untersagt Microsoft den Zugriff auf und die Benutzung von Kundendaten für Zwecke, die nicht durch geschäftliche Erfordernisse bedingt sind. Erlaubt sind demnach Handlungen im Zusammenhang mit der Administration der Datenbanken oder in Antwort auf Supportanfragen des Kunden, sofern ein solcher Zugang erforderlich ist, um Dienste und andere für die Leistungserstellung benutzte Microsoft-Produkte und -Dienste zu verbessern oder um auf rechtliche Anfragen zu antworten.

Zugang für Entwicklung und Support: Softwareentwicklungsmitarbeiter und Mitarbeiter im Kundensupport verfügen nicht über Administratorrechte für die Microsoft Online Services-Systeme.

Kontrollmaßnahmen, die auf jede Zugriffskategorie zutreffen: Microsoft wendet auf den Zugang zur Microsoft Online Services-Infrastruktur und zu Kundendaten strikte Kontrollen an. So werden z.B. alle neuen Microsoft-Mitarbeiter in den USA vor der Einstellung durch Microsoft einer Sicherheitsprüfung unterzogen. Außerdem müssen Microsoft-Mitarbeiter, die über Zugang zur Microsoft Online Services-Infrastruktur verfügen, ein Anmeldeformular ausfüllen und geschäftlich begründen, warum sie Zugang benötigen. Bevor der Zugang gewährt wird, muss der Manager der Person die Zugangsanfrage prüfen und genehmigen. Die Zugangsberechtigungen werden regelmäßig überprüft, um sicherzustellen, dass

nur diejenigen Benutzer Zugang zu den Systemen erhalten, die ihn aus nachweislichen und fortbestehenden geschäftlichen Gründen benötigen. Wenn Microsoft-Mitarbeiter das Unternehmen verlassen, durchlaufen sie ein Austrittsverfahren, bei dem ihr logischer und physischer Zugang zur Microsoft Online Services-Infrastruktur aufgehoben wird.

Ferner setzt Microsoft für den Zugriff auf die Infrastruktur, auf der Microsoft Online Services gehostet werden, Smartcards (Zweifaktorauthentifizierung) oder RSA-Tokens voraus. Bei der Zweifaktorauthentifizierung werden zwei Faktoren genutzt, um die Identität eines Benutzers zu bestätigen. Davon ist der eine ein Passwort oder eine PIN (d.h. etwas, was dem Benutzer bekannt ist), während der andere ein physisches Gerät im Besitz des Benutzers ist (d.h. eine Smartcard oder ein RSA-Token). Dies bietet einen stärkeren Schutz vor Angriffen wie Passwortschneidung (d.h. selbst, wenn das Passwort eines Benutzers ausgespäht wird, benötigt der Hacker Zugriff auf das physische Gerät, um Zugang zum System zu erlangen. Ebenso müsste beim Verlust des physischen Gerätes (Smartcard oder RSA-Token) das Passwort des Benutzers bekannt sein, damit jemand Zugriff auf das System erhielte.)

Frage: Welche Sicherheitsprüfungen führt Microsoft bezüglich Personen durch, die Administratorrechte erhalten? Tauschen Sie die Sicherheitsprüfungen mit Kunden aus?

Microsoft hat festgestellt, dass es einen wichtigen Teil des Auswahlprozesses darstellt, Kandidaten einer Sicherheitsprüfung zu unterziehen – unabhängig davon, über welche Zugriffsrechte auf die Microsoft Online Services-Infrastruktur der Mitarbeiter verfügt. Die Einholung von umfassenden, für den Job relevanten Informationen hilft Microsoft, eine leistungsfähige Belegschaft einzustellen und zu halten. Sicherheitsprüfungen umfassen unter Umständen Informationen bezüglich der Ausbildung und des beruflichen Werdegangs von Kandidaten sowie deren polizeiliches Führungszeugnis und Bonitätsprüfungen. In den USA beginnt kein Kandidat oder Angestellter mit der Arbeit oder erhält einen Auftrag, solange nicht die erforderlichen Sicherheitsprüfungen erfolgreich bestanden wurden. Um die Privatsphäre seiner Mitarbeiter zu schützen, gibt Microsoft die Ergebnisse von Sicherheitsprüfungen nicht an Kunden weiter.

FRAGE: Erfüllen die Dienste die Vorgaben des Gramm Leach Bliley Acts (GLBA)?

Microsoft Online Services hilft Kunden, die Sicherheitsanforderungen des GLBA zu erfüllen, indem es technische und organisationale Sicherungen zur Verfügung stellt, mit denen Kunden die Sicherheit gewährleisten und unberechtigte Nutzung unterbinden können. Microsoft stellt auf Anfrage eine Zusammenfassung der Zertifizierung durch einen unabhängigen Prüfer zur Verfügung. Microsoft Office Live Meeting verfügt ebenfalls über Benachrichtigungsfunktionen, die Kunden bei der Einhaltung von GLBA unterstützen können.

FRAGE: Erfüllen die Microsoft Online Services die Vorgaben des HIPAA (Health Insurance Portability and Accountability Act)?

Manche Microsoft Online Services verfügen über Leistungsmerkmale, die Kunden bei der Einhaltung der HIPAA-Vorgaben unterstützen; der Kunde muss jedoch die Einhaltung selber sicherstellen, indem er die Leistungsmerkmale in die Richtlinien und Abläufe seiner Organisation integriert. Microsoft Online Services dienen als Informationskanal, der technische und organisationale Sicherheitsmaßnahmen umfasst, durch die Kunden die Sicherheit gewährleisten und unberechtigte Benutzung unterbinden können; Microsoft-Mitarbeiter greifen in der Regel nicht auf Kundendaten zu. Weitere Informationen

über unsere Richtlinien hinsichtlich der Sammlung, Benutzung und des Austauschs von persönlichen Daten stehen in den [Microsoft Online Services-Datenschutzbestimmungen](#) zur Verfügung.

FRAGE: Ist Microsoft bereit, ein HIPAA Business Associates Agreement (BAA) zu unterschreiben?

Microsoft unterschreibt keine Business Associate Agreements oder andere HIPAA-Einhaltungsdokument für Microsoft Online Services. Microsoft Online Services dienen wie in den HIPAA-Regulierungen beschrieben lediglich als Kanal für die Informationen des Kunden und können deshalb benutzt werden, ohne dass hierzu ein BAA unterschrieben werden muss.

FRAGE: Erfüllen die Microsoft Online Services den Payment Card Industry Data Security Standard (PCI DSS)?

Microsoft Online Services-Kunden können mit Kreditkarte für die von ihnen bezogenen Dienste bezahlen. Microsoft verarbeitet diese Informationen in Übereinstimmung mit den PCI-Richtlinien und die Systeme, die mit Kundenkreditkarten umgehen, sind Level One PCI Compliant.

FRAGE: Erlaubt es Microsoft Kunden, Microsoft Online Services zu prüfen?

Microsoft prüft und überwacht die Microsoft Online Services-Umgebungen regelmäßig, um sicherzustellen, dass die Kontrollmaßnahmen angemessen sind und funktionieren. Außerdem werden diese Umgebungen Prüfungen durch externe, unabhängige Anbieter unterzogen, um die internen Prozesse und Systeme von Microsoft zu bestätigen. Die interne Überwachung durch Microsoft umfasst die automatische Compliance-Überwachung der Infrastruktur (z.B. Schwachstellenanalysen, Penetrationstests und Prüfungen von Prozess- und Personalkontrollen). Das von Drittparteien durchgeführte Validierungsprogramm der Microsoft Online Services beinhaltet unabhängige Prüfungen, die jährlich zur Bestätigung der Sicherheit durchgeführt werden.

Aus Sicherheitsgründen erlaubt es Microsoft Microsoft Online Services-Kunden nicht, seine physischen oder logischen Umgebungen zu prüfen.

FRAGE: Welcher Art von unabhängigen Prüfungen und/oder Zertifizierungen werden die Microsoft Online Services unterzogen? Wie breit ist der Anwendungsbereich der Dienste, die durch diese Zertifizierungen abgedeckt werden und wie oft werden die Prüfungen durchgeführt?

Die folgende Tabelle stellt den Prüfungs- und Zertifizierungsstatus verschiedener Microsoft Online Services im Juni 2009 dar:

Dienst/Prüfung durch Drittanbieter	Business Productivity Online Suite - Standard (außer Forefront Online Security for Exchange & Live Meeting)	Forefront Online Security for Exchange	Live Meeting
Cybertrust	JA	NEIN	JA
SAS 70 Typ II	ERWARTET	NEIN	NEIN
ISO 27001	ERWARTET	ERWARTET	ERWARTET

Rechenzentrum/ Prüfung durch Drittanbieter	BPOS-S (außer FOSE & LM)	FOSE	LM
Cybertrust	JA	NEIN	JA
SAS 70 Typ II	JA	JA*	JA*
ISO 27001	JA	JA (außer Rechenzentren von Drittanbietern)	JA*

*Microsoft hostet diese Dienste unter Umständen in Rechenzentren, die von Drittanbietern betrieben werden. Falls dies der Fall ist, befindet sich die angegebene Zertifizierung im Besitz des Drittanbieters.

FRAGE: Wo kann ich weitere Informationen über SAS 70 erhalten?

SAS 70 ist ein Prüfstandard, der vom American Institute of Certified Public Accountants (AICPA) definiert wird und der für Dienstleistungsunternehmen ausgelegt ist. Dienstleistungsunternehmen sind typischerweise Körperschaften, die Auslagerungsdienste anbieten, die die Kontrollumgebung ihrer Kunden beeinflussen. Hierzu gehören zum Beispiel Unternehmen, die Schadensmeldungen für Versicherungen und Krankenversicherungen bearbeiten, gehostete Rechenzentren, Anwendungsdienstleister und Anbieter von verwalteter Sicherheit. Bei SAS 70 handelt es sich um eine unabhängige Bestätigung der Einhaltung von Sicherheitskontrollen sowie der Wirksamkeit von Sicherheitskontrollen. SAS 70-Prüfungen werden von Deloitte & Touche (D&T) für Microsoft durchgeführt. SAS 70-Prüfungen werden einmal pro Jahr durchgeführt. D&T prüft die Kontrollen, inklusive dem Entwurf von Kontrollen und der Beweisanalyse für einen bestimmten Zeitraum. D&T erstellt den Prüfbericht, in dem neben den Prüfergebnissen für die Kontrollen auch die Kontrollen selbst einer Einschätzung unterzogen werden. Weitere Informationen zu der Norm und den verschiedenen Prüfarten stehen auf www.aicpa.org oder von dem Prüfunternehmen des Kunden zur Verfügung.

FRAGE: Deckt die SAS 70-Prüfung auch die geschäftliche Kontinuität ab?

Obwohl die Richtlinien des American Institute of Certified Public Accountants (AICPA) bei der SAS 70-Prüfung die Kontinuität explizit ausschließen, hat Microsoft ein stabiles Kontinuitätsprogramm eingerichtet, das die zügige Wiederherstellung von Diensten gewährleisten soll.

Datenschutz

FRAGE: Auf welche Weise benachrichtigt Microsoft seine Kunden, falls Microsoft gerichtlich dazu aufgefordert wird, Kundeninformationen offenzulegen?

Microsoft ist der Meinung, dass Kunden selbst die Kontrolle über ihre Daten behalten sollten. Wenn also Vollzugsbehörden Microsoft direkt nach Daten fragen, die es im Namen seiner Unternehmenskunden auf seinen Systemen hostet, versucht Microsoft soweit wie möglich die rechtlichen Prozesse an den Kunden weiterzuleiten, damit dieser selbst entscheiden kann, wie er reagieren möchte. Obwohl dies auf der Grundlage von internen Richtlinien die Position von Microsoft darstellt, wird es nicht immer möglich sein, die Anfrage an den Kunden weiterzuleiten, insbesondere dann, wenn die Rechtslage es den Vollzugsbehörden erlaubt, die Daten direkt von Microsoft zu verlangen.

Wenn Microsoft gezwungen ist, stattzugeben, unternimmt es kommerziell angemessene Anstrengungen, den Kunden darüber zu benachrichtigen, dass seine Daten angefordert wurden, vorausgesetzt, eine solche Benachrichtigung ist rechtmäßig. Die Benachrichtigung bietet dem Kunden die Möglichkeit, zum Schutze seiner Daten einzugreifen. Es kann jedoch vorkommen, dass es Microsoft rechtlich nicht gestattet ist, eine Benachrichtigung weiterzugeben. Wenn es darüber hinaus keinen stichhaltigen Grund gibt, warum Microsoft dem legalen Prozess widersprechen sollte, müssten die Freigabebeforderung erfüllt werden.

Microsoft stellt Kundendatensätze nur dann zur Verfügung, wenn es rechtlich dazu verpflichtet ist, und beschränkt die Weiterleitung auf diejenigen Informationen, die es freigeben muss. Die einzige Ausnahme dieser Regel bestünde in Fällen, in denen die Informationsweitergabe an Vollzugsbehörden oder andere Parteien unter Umständen stattfindet, bei denen Microsoft in dem begründeten Glauben handelt, dass aufgrund eines Notfalls, bei dem ein Todes- oder Verletzungsrisiko besteht, die Daten unverzüglich offengelegt werden müssen.

FRAGE: Wie hilft Microsoft Kunden, die auf eine Anfrage auf den Zugriff auf Informationen im Rahmen eines Gerichtsverfahrens antworten müssen?

Microsoft Online Services-Kunden haben die Kontrolle über ihre eigenen Daten und sollten selbst in der Lage sein, auf die meisten elektronischen Anfragen auf den Zugriff auf Informationen im Rahmen eines Gerichtsverfahrens zu antworten. Microsoft bietet als Erweiterung einen Nachrichtenarchivierungsdienst, der Kunden hierbei unterstützen kann.

FRAGE: Manche Kunden müssen Sicherungskopien für eine bestimmte Anzahl von Jahren aufbewahren. Unterstützt Microsoft diese Funktionalität?

Ja. Dokumente, die gespeichert werden müssen, können auf einer SharePoint-Site als Teil des SharePoint Online-Dienstes gespeichert werden. Ferner können Archivierungslösungen, die mit dem Exchange Online-Dienst verknüpft sind, direkt von Microsoft beschafft werden. Die Archivierungslösungen stellen, wenn sie richtig konfiguriert sind, einen Datensatz mit allen E-Mails zur Verfügung, die von dem Exchange Online-Dienst eines Kunden gesendet oder empfangen wurden, und bieten die Möglichkeit, über Postfächer hinweg nach Informationen zu suchen und andere leistungsfähige Archivierungsfunktionen zu nutzen.

Microsoft speichert als Teil seiner Standardabläufe rollierend Sicherungskopien der in den Microsoft Online Services enthaltenen Daten für einen begrenzten Zeitraum. Es wird jedoch darauf hingewiesen, dass dies zum Zweck der Dienstkontinuitätssicherung geschieht und nicht anstelle einer Archivierungslösung benutzt werden sollte. Die Aufbewahrungsdauer der Sicherungskopien ist kurz und Sicherungskopien können in der Regel nicht wiederhergestellt werden.

Dienstkontinuität

FRAGE: Welche Redundanz- bzw. Ausfallfunktionalitäten sind Bestandteil von Microsoft Online Services? Werden Daten repliziert und gesichert?

Alle Dienste werden aus zwei Rechenzentren angeboten, zwischen denen eine Replikation stattfindet. Außerdem gibt es in jedem Rechenzentrum mehrfache Kopien der Daten. Bei ernststen Zwischenfällen sichert Microsoft die Dienstkontinuität, indem auf das alternative Rechenzentrum geschaltet wird.

FRAGE: Gibt es bei Microsoft ein formalisiertes Kontinuitätsprogramm?

Microsoft verfügt über stabile Dienstkontinuitätsprogramme für Microsoft Online Services. Diese Programme basieren auf den bewährten Vorgehensweisen in der Branche und ermöglichen es, abonnierte Dienste zügig wiederherzustellen.

FRAGE: Kann jeder Dienst im Fall eines Ausfalls wieder hergestellt werden?

Ja, alle Dienste verfügen über Redundanz und Ausfallsicherheit, um sicherzustellen, dass signifikante oder ernste Ausfälle minimiert werden.

FRAGE: Was ist ein Recovery Time Objective (RTO)?

Bei einem RTO handelt es sich um den Zeitraum, innerhalb dessen Systeme, Anwendungen oder Funktionen nach einem Ausfall wieder hergestellt werden müssen (z.B. innerhalb eines Arbeitstages). RTOs werden oft als Grundlage für die Entwicklung von Wiederherstellungsstrategien verwendet und dienen als Entscheidungsgrundlage dafür, ob die Wiederherstellungsstrategien im Fall eines Ausfalls zur Anwendung kommen sollen oder nicht.

FRAGE: Was ist ein Recovery Point Objective (RPO)?

Bei einem RPO handelt es sich um die maximale Datenmenge, die ein Unternehmen während eines Zwischenfalls verlieren darf.

FRAGE: Welche Art von Notfall-Übungen führt Microsoft für Microsoft Online Services durch?

- **Theoretische Übung** – Die Teilnehmer prüfen und besprechen die Prozesse, Abläufe und Aufgaben, die sie im Notfall durchführen würden, ohne tatsächlich die Handlungen durchzuführen. Hierbei können die Benutzer prognostizieren, wie die Wiederherstellungslösung überprüft werden würde, und sicherstellen, dass der Inhalt ihres Plans umfassend und vollständig ist.
- **„Alternativer Standort“-Übung** – Teilnehmer führen die Prozesse und Aufgaben in einer kontrollierten Umgebung so aus, wie sie es im Fall eines Ausfalls täten. Bei dieser Übungsart wird die Lösung am alternativen Wiederherstellungsstandort geprüft und es wird festgestellt, ob der Dienst produktiv ist und wie geplant funktioniert.
- **„Geo-diverse“-Übung** – Die Teilnehmer führen die Prozesse und Aufgaben für eine Cloud-Wiederherstellungslösung oder eine Wiederherstellungslösung mit mehreren Standorten durch. Der Prüf- und Bestätigungsprozess ist derselbe wie oben, aber mit mehr Komplexität und Interaktion, weil er sich auf manuelle Interventionslösungen bezieht. Automatisierte Geo-diversity-Lösungen sind leichter zu prüfen und zu pflegen und erfordern weniger Arbeit.

FRAGE: Wie wird die Wiederherstellungslösung geprobt?

Alle Dienste durchlaufen einen Dreiphasenprozess mit den Phasen Vor der Übung, Während der Übung und Nach der Übung. Dies hilft sicherzustellen, dass der Umfang und das Szenario klar definiert sind, die Übung durchgeführt wird und Probleme bei Bedarf schnell identifiziert und durch Ergänzungen und Änderungen der Dokumentation und Lösung gelöst werden.

Interne Prüfungen finden regelmäßig statt, um die ordnungsgemäße Funktionsweise der Dienste sicherzustellen. Hierzu gehört, die Datenübertragung vom Haupt- an sekundäre bzw. geo-diverse

Standorte sowie die Funktionalität von System und Dienst zu prüfen, und ferner festzustellen, ob die Lösung die derzeit angebotenen Fähigkeiten wiedergibt.

FRAGE: Hat der Kunde im Fall von BPOS Standard die Möglichkeit, an der Übung teilzunehmen?

Nein, aufgrund der Beschaffenheit der Produktiv- und Wiederherstellungsumgebung ist es nicht möglich, Übungen mit Kunden durchzuführen.

FRAGE: Wie werden Mängel behoben, die während einer Dienstkontinuitätsübung entdeckt wurden?

Nach jeder Prüfung aller Dienste wird eine Phase „Nach der Übung“ durchgeführt, bei der alle Probleme identifiziert werden, die sich in Folge des Ereignisses ergeben haben. Die Lösungen und Zeiträume werden festgelegt, Eigentümer werden identifiziert und das Service Continuity Management Team steuert die Behebung der Probleme. Hierzu gehören u.U. die Aktualisierung der Dokumentation für die Kontinuitätspläne sowie Trainingsmaßnahmen oder Änderungen der Lösung selbst.

FRAGE: Gibt es Pläne für die Lösung?

Ja, jede Lösung verfügt über einen Wiederherstellungsplan und wird aktualisiert, wenn neue Funktionen eingeführt oder bedeutende Änderungen durchgeführt werden.

FRAGE: Unterscheidet sich das RTO- bzw. RPO-Dienstniveau von Kunde zu Kunde?

Nein. Alle RTOs und RPOs werden im Voraus für jeden Dienst festgelegt und gelten gleichermaßen für alle Kunden. Ziel ist, die Konsistenz der Methodik, der Lösungsarchitektur und der Skalierbarkeit sicherzustellen.

FRAGE: Ist der Wiederherstellungsstandort an ein anderes Strom- und Datennetzwerk angebunden als der Hauptstandort?

Ja. Alle Alternativstandorte befinden sich in anderen Regionen, um sicherzustellen, dass Ausfälle möglichst auf den Hauptstandort begrenzt bleiben und den sekundären Standort nicht beeinflussen.