

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Whitepaper

Veröffentlicht: Juni 2009

Die Microsoft Business Productivity Online Standard Suite von Microsoft® Online Services bietet effiziente, ökonomische und skalierbare Dienste für Kommunikation und Zusammenarbeit für Ihr Unternehmen.

Neben Zuverlässigkeit, Kontinuität und Datenschutz steht die Sicherheit der Onlineumgebung ganz weit oben auf der Liste der Kundenanforderungen. In diesem Dokument wird beschrieben, wie die Sicherheit als zentrales Merkmal bei allen Aspekten der Business Productivity Online Standard Suite berücksichtigt wurde.

Der Microsoft-Ansatz, die Dienste und Kundendaten kontinuierlich zu schützen, ist wesentlicher Bestandteil des Risikomanagementprogramms (RMP) von Microsoft. Das Risikomanagementprogramm zielt darauf ab, im Bereich der Dienste die Praktiken stärker zu verankern, die von der Microsoft Trustworthy Computing-Initiative definiert wurden. Bei dieser Initiative handelt es sich um einen langfristigen, kollaborativen Ansatz, um eine sichere, geschützte und zuverlässige Computernutzung zu ermöglichen.

Microsoft schafft mit den Online Services bei seinen Kunden Vertrauen, indem es die Einhaltung von Industriestandards für Dienstvorgänge durch regelmäßige Prüfungen und Zertifizierung durch Dritte sichergestellt.

Die neuesten Informationen zur Business Productivity Online Standard Suite und zu weiteren Microsoft Online Services finden Sie unter [Microsoft Online Services](#).

Die in diesem Dokument enthaltenen Informationen stellen die aktuellen Kenntnisse von Microsoft Corporation zu den erläuterten Problemen zum Zeitpunkt der Veröffentlichung dar. Da Microsoft auf sich ändernde Marktbedingungen reagieren muss, folgen aus den genannten Informationen keinerlei Verbindlichkeiten für Microsoft. Microsoft kann keine Garantie für die Gültigkeit von Informationen übernehmen, die nach dem Zeitpunkt der Veröffentlichung vorgestellt werden.

Dieses Whitepaper dient nur zu Informationszwecken. MICROSOFT SCHLIESST FÜR DIE INFORMATIONEN IN DIESEM DOKUMENT JEDE GEWÄHRLEISTUNG AUS, SEI SIE AUSDRÜCKLICH, KONKLUDENT ODER GESETZLICH GEREGLT.

Für die Einhaltung aller zutreffenden Urheberrechte ist der Benutzer verantwortlich. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder in einem Datenabfragesystem gespeichert oder darin eingelesen oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies geschieht.

Microsoft kann Inhaber von Patenten, Patentanträgen, Marken, Urheberrechten oder anderem geistigen Eigentum sein, die den Inhalt dieses Dokuments betreffen. Die Bereitstellung dieses Dokuments gewährt keinerlei Lizenzrechte an diesen Patenten, Marken, Urheberrechten oder anderem geistigen Eigentum, es sei denn, dies wurde ausdrücklich durch einen schriftlichen Lizenzvertrag mit Microsoft vereinbart.

Sofern nicht anders angegeben, sind die Unternehmen, Organisationen, Produkte, Domännennamen, E-Mail-Adressen, Logos, Personen, Orte und Ereignisse in den hier enthaltenen Beispielen frei erfunden. Jede Ähnlichkeit mit tatsächlichen Firmen, Organisationen, Produkten, Domänen, E-Mail-Adressen, Logos, Personen, Orten oder Ereignissen ist rein zufällig.

© 2009 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, Active Directory, Exchange, Forefront, SharePoint und Windows Server sind Marken der Microsoft-Unternehmensgruppe.

Alle weiteren Marken sind Eigentum der jeweiligen Eigentümer.

Inhalt

Kurzfassung	1
Warum Onlinedienste?	2
Warum Onlinedienste von Microsoft?	3
Die Grundlage von Microsoft Online Services: Trustworthy Computing	4
Die Trustworthy Computing-Initiative	4
Entwickeln sicherer Dienste: Security Development Lifecycle (SDL)	5
Vertrauen schaffen und aufrechterhalten: Das Risikomanagementprogramm von Microsoft Online Services	7
Zielsetzungen des Risikomanagementprogramms	7
Erfolgskriterien des Risikomanagementprogramms	7
Kerndisziplinen des Risikomanagements.....	8
Sicherheit	9
Ein umfassender, kontinuierlicher Prozess	9
Physische Sicherheit	9
Carrier-Class-Datencenter.....	10
Weltweite Standorte von Datencentern	10
Sicherheit für das Datencenterpersonal	10
Sicherheit bei Entwurf und Vorgängen des Netzwerks	11
Modernste Hardware	11
Logische Sicherheit	11
Features von Microsoft Online Services.....	11
Die Infrastruktur von Microsoft Online Services	13
<i>Systemverwaltung und Zugriffssteuerung</i>	13
Das Netzwerk von Microsoft Online Services	15
Schutz vor bösartiger Software	15
Operations von Weltklasse.....	16
Überwachung und Risikominderung	17
Integration von Sicherheit und Operations	18
Umsetzung der Prinzipien des Risikomanagements.....	19
Verwaltung von Sicherheitsvorfällen	21
Sicherheitsuntersuchung	21
Datenschutz bei Microsoft Online Services	23
Datenschutz schon beim Entwurf	23
Spezielle Datenschutzpraktiken: Marketing und Werbung sowie Tests	23
Anbieter und Partner	24
Anbieter	24
Partner	24
Zugriff, Sicherheit, Datenintegrität und Erzwingung.....	24
Kundenanleitung.....	24
Internationale Datenübertragung.....	26

Verwaltung der Dienstkontinuität	27
Messagingkontinuität durch Archivierung.....	27
Datenspeicher	27
Verfügbarkeit und Kontinuität	29
99,9-prozentige Zuverlässigkeit.....	29
Vermeiden von Ressourceneinschränkungen durch Skalierbarkeit.....	29
Dedizierter Support.....	29
Selbsthilfe gestützt durch kontinuierlichen Personalsupport	30
Kompatibilität	31
Auf Standards basierende Kompatibilitätsverwaltung.....	31
Kompatibilitätsverwaltungsprogramm von Microsoft Online Services.....	31
Das Kompatibilitätsframework von Microsoft Online Services	32
Bewertungen und Überprüfungen der Kompatibilität	33
Unabhängige Zertifizierung	34
Demonstrieren der Kompatibilität	34
Statement of Auditing Standard (SAS) 70	34
ISO 27001.....	34
Verizon Security Management Program – Service Provider Certification.....	35
Aktueller und zukünftiger Status von Online Services-Zertifizierungen durch Dritte.....	35
Weitere Informationen	36
Microsoft Online Services.....	36
Sicherheit und Dienstkontinuität.....	36
Datenschutz.....	36
Kompatibilität	36

Kurzfassung

Mit diesem Dokument sollen Fragen zur Sicherheit und Zuverlässigkeit der Business Productivity Online Standard Suite von Microsoft® Online Services beantwortet werden. Dazu werden die Funktionen, Technologien und Prozesse beschrieben, die für das Vertrauen in die Business Productivity Online Standard Suite sorgen und erstklassige Onlinedienste für Ihr Unternehmen bereitstellen. Es wird erläutert, wie die umfassenden Erfahrungen von Microsoft beim Erstellen und Betreiben von Unternehmenssoftware zur erprobten Zuverlässigkeit und Vertrauenswürdigkeit der Angebote von Microsoft Online Services geführt haben. In diesem Dokument wird beschrieben, wie Microsoft die folgenden Aspekte umsetzt:

- Verwaltung von Sicherheit, Datenschutz und Kontinuität der Online Services mit einem robusten und ausgereiften Kompatibilitätsverwaltungsprogramm
- Orientierung an Industriestandards für Sicherheit und Zuverlässigkeit
- Veranlassung regelmäßiger Überprüfungen und Tests durch unabhängige anerkannte Organisationen

In den richtigen Händen bieten Anwendungen für Messaging und Zusammenarbeit mehr Sicherheit, Verfügbarkeit und Skalierbarkeit, als wenn Sie die Ausgaben und den Aufwand für das Betreiben dieser Dienste selbst übernehmen würden.

Warum Onlinedienste?

*Fragen Sie
Ihren
Onlinedienstanbieter:*

Wie sicher?

Wie vertraulich?

Wie verfügbar?

... Und wie

Schlüsselanwendungen wie Tools für Messaging, Zusammenarbeit von Mitarbeitern und Gruppen sowie Onlinekonferenzdienste bilden die Grundlage für Unternehmen jeder Größe und in allen Branchen. Diese Anwendungen sind für alltägliche Vorgänge in Ihrem Geschäft notwendig, können jedoch in Anschaffung und Betrieb teuer sein. Diese wichtigen Kommunikationstools erfordern Personal mit speziellen Fachkenntnissen jenseits der Schlüsselanforderungen für Ihr Unternehmen, können einen beachtlichen Mehraufwand bedeuten und müssen regelmäßig gewartet und überwacht werden, damit ein sicherer und zuverlässiger Betrieb gewährleistet ist.

Bis vor kurzem gab es wenig Alternativen zum Betrieb eigener IT-Anwendungen und -Dienste vor Ort. Dank der Entwicklung webbasierter Technologien, mit denen Dienstleister das Hosten übernehmen können, ergeben sich jedoch neue Möglichkeiten, jederzeit genau auf die Dienste zuzugreifen, die Sie benötigen, ohne sie selbst bereitzustellen und betreiben zu müssen.

Zu den unmittelbaren Vorteilen von webbasierten Diensten bzw. Onlinediensten zählen niedrigere Gesamtbetriebskosten: Es muss weder spezialisiertes Personal eingestellt werden, noch müssen Geräte aufgestellt werden. Zudem muss keine Serversoftware verwaltet und betrieben werden. Die Dienste lassen sich bequem den Geschäftsanforderungen entsprechend skalieren. Sie sind niemals unter- oder überversorgt, und Ihre „virtuelle“ IT-Onlineabteilung wächst mit Ihren sich ändernden Anforderungen und passt sich diesen an.

Allerdings erfordert das Übergeben der Kontrolle Ihrer IT-Dienste an einen Onlinedienstleister viel Sorgfalt und wirft einige unmittelbare Fragen auf:

- Wie erfahren ist mein Onlinedienstleister?
- Wie kann ich sicher sein, dass meine Daten vertraulich behandelt werden und nur die richtigen Personen darauf zugreifen können?
- Wie sicher sind meine Daten?
- Sind meine Daten verfügbar, wenn ich sie benötige?
- Sind meine Dienste für E-Mails und Zusammenarbeit einsatzbereit, wenn ich sie benötige?
- Wie kann ich sicher sein, dass der Dienst so zuverlässig und sicher ist, wie es der Dienstleister behauptet?

Microsoft Online Services bietet eine Auswahl gehosteter Dienste für Kommunikation und Zusammenarbeit, die flexibel und mit geringen Gemeinkosten verbunden sind.

Warum Onlinedienste von Microsoft?

Die Business Productivity Online Standard Suite ist eine Zusammenstellung von Microsoft Online Services – Softwaredienste, die auf Abonnements basieren, von Microsoft gehostet und durch Partner vertrieben werden. Die Onlinedienste werden in einer Umgebung mit umfassenden Features und Funktionen betrieben, mit denen Sie die für Ihre Geschäftsanwendungen gesetzten Ziele bezüglich Sicherheit und Verfügbarkeit erreichen und in vielen Fällen sogar übertreffen können. In modernsten Datacentern werden hochsichere Server gehostet, die mit erprobten, branchenführenden bewährten Methoden betrieben werden. Mit diesen und anderen Features der Business Productivity Online Standard Suite können Sie Ihre Daten vom Desktop bis zum Datacenter schützen. Zudem steht Ihnen qualifiziertes Supportpersonal von Weltklasse mit Rat und Tat zur Seite.

Bei der Registrierung für die Business Productivity Online Suite können Sie eine Reihe ausgereifter Unternehmensanwendungen mit wichtigen Features, wie E-Mail, Zusammenarbeit, Sofortnachrichten und webbasierte Konferenzdienste, auswählen.

Microsoft verfügt über langjährige Erfahrung beim Entwerfen von Hostingbereitstellungen für Internetdiensteanbieter, bei denen diese ausgereiften Unternehmensanwendungen als webbasierte Dienste ausgeführt und Geschäftskunden angeboten werden. Diese Erfahrung fließt in den allgemeinen Entwurf der Architektur von Microsoft Online Services ein.

Die Business Productivity Online Standard Suite von Microsoft umfasst die folgenden Dienste:

- **Microsoft Exchange Online** – Eine gehostete Messaginglösung für Unternehmen basierend auf Microsoft Exchange Server 2007. Exchange Online bietet Unternehmen die notwendige E-Mail-Sicherheit, mobilen Zugriff für Mitarbeiter sowie Betriebseffizienz für das IT-Personal.
- **Microsoft SharePoint® Online** – Eine gehostete Zusammenarbeitslösung für Unternehmen basierend auf Microsoft Office SharePoint Server 2007. SharePoint Online bietet Unternehmen einen sicheren, zentralen Ort, an dem Mitarbeiter effizient mit Teammitgliedern zusammenarbeiten, nach Ressourcen in der Organisation suchen, Inhalte und Workflows verwalten sowie geschäftliche Einsichten für besser fundierte Entscheidungen erhalten können.
- **Microsoft Office Communications Online** – Eine von Microsoft gehostete Lösung für Sofortnachrichten und Anwesenheitsinformationen basierend auf Microsoft Office Communications Server 2007. Office Communications Online bietet Unternehmen eine Umgebung mit mehr Sicherheit als öffentliche Sofortnachrichtentools, um die Zusammenarbeit in Echtzeit sowie das Arbeiten in international verteilten Teams zu ermöglichen.
- **Microsoft Office Live Meeting** – Eine von Microsoft gehostete Webkonferenzlösung, mit der Unternehmen von praktisch jedem Ort aus zusammenarbeiten können. Lediglich ein Computer mit einer Internetverbindung und grundlegender Software ist erforderlich, damit Mitarbeiter intern zusammenarbeiten sowie Kunden und Partner extern durch Echtzeitbesprechungen, Schulungssitzungen und Veranstaltungen einbeziehen können.

Das Ergebnis ist ein Paket aus Microsoft Online Services für Unternehmen, die einfach skaliert werden können – und das zu klaren und kalkulierbaren Preisen. Darüber hinaus werden die Dienste mit fortlaufenden Verbesserungen und Technologieaktualisierungen ohne Zusatzkosten bereitgestellt.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Die Grundlage von Microsoft Online Services: Trustworthy Computing

Microsoft Online Services, einschließlich der Onlinedienste in der Business Productivity Online Standard Suite, basiert auf ausgereiften Praktiken bezüglich Softwareentwurf, Entwicklung, Tests, Betrieb und Verwaltung. Diese orientieren sich eng an den Grundprinzipien, die den Microsoft-Ansatz für Sicherheit, Datenschutz und allgemeine Unternehmenspraktiken charakterisieren.

Die Trustworthy Computing-Initiative

2002 legte Bill Gates den Grundstein für die Trustworthy Computing-Initiative, die unternehmensweite Bemühung, „...*Vertrauen in unsere Produkte und Dienstleistungen zu schaffen*“. Bill Gates legte die wichtigsten Aspekte der Initiative fest, die den Microsoft-Ansatz für das Erstellen von Software und Dienstleistungen verkörpern sollten:

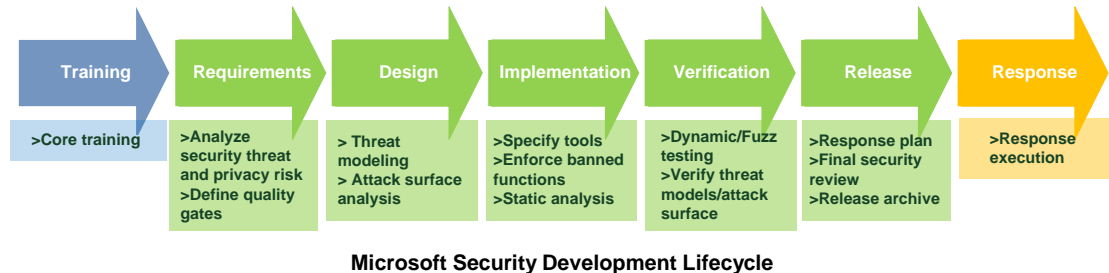
- **“Verfügbarkeit:** *Unsere Produkte sollten immer verfügbar sein, wenn unsere Kunden sie benötigen. Systemausfälle sollten der Vergangenheit angehören, da die Softwarearchitektur Redundanz und automatische Wiederherstellung unterstützt. Die Selbstverwaltung sollte in fast allen Fällen eine Wiederaufnahme des Diensts ohne Benutzereingriff ermöglichen.*
- **Sicherheit:** *Die Daten, die im Auftrag unserer Kunden von unserer Software und unseren Diensten gespeichert werden, sollten vor Beschädigung geschützt sein und nur in vorgesehener Weise verwendet und geändert werden. Sicherheitsmodelle sollten für Entwickler einfach zu verstehen und in ihre Anwendungen zu integrieren sein.*
- **Datenschutz:** *Benutzer sollten die Kontrolle darüber haben, wie ihre Daten verwendet werden. Die Richtlinien für die Verwendung von Informationen sollten für den Benutzer verständlich sein. Benutzer sollten bestimmen können, wann und ob sie Informationen erhalten, um ihre Zeit bestmöglich nutzen zu können. Es sollte für Benutzer einfach sein, über die angemessene Verwendung ihrer Informationen zu bestimmen, einschließlich der Verwendung der von ihnen gesendeten E-Mails.”*

Das allgemeine Ziel von Trustworthy Computing, inzwischen ein Unternehmensgrundsatz bei Microsoft, ist eine sichere, geschützte und zuverlässige Computernutzung. Trustworthy Computing bedeutet nicht nur, die Computernutzung grundsätzlich sicherer zu machen, sondern auch, für mehr Verlässlichkeit und Verfügbarkeit zu sorgen, während gleichzeitig der Schutz der Daten des Kunden sichergestellt wird.

Sicherheit ist ein wesentliches Element der langen Microsoft-Geschichte von Softwareentwicklung und Unternehmenskultur.

Entwickeln sicherer Dienste: Security Development Lifecycle (SDL)

Der Microsoft Security Development Lifecycle (Entwicklungszyklus für sichere Software), der branchenführende Prozess zur Gewährleistung von Softwaresicherheit, wird bei Microsoft Online Services für Entwicklung, Bereitstellung und Verwaltung angewendet. Wie die Trustworthy Computing-Initiative ist SDL eine unternehmensweite Initiative von Microsoft und seit 2004 verbindliche Richtlinie. SDL hat beim Integrieren von Sicherheit und Datenschutz in Microsoft-Software und -Kultur eine wichtige Rolle gespielt. Dabei werden Sicherheit und Datenschutz von Beginn an während des gesamten Entwicklungsprozesses berücksichtigt.



Sämtliche Microsoft-Software und -Dienste in Online Services werden dem SDL-Prozess entsprechend erstellt. Bei SDL werden Bedrohungsmodelle für jede Komponente entwickelt, um jede erkannte Bedrohung anhand einer oder mehrerer Risikokategorien zu bewerten:

- **Identitätsspoofing** – Angriffe, bei denen ein Benutzer oder Server sich als gültiger Benutzer oder gültiges Gerät innerhalb der Umgebung ausgibt
- **Manipulation von Daten** – Angriffe, bei denen Daten mit böswilliger Absicht geändert werden oder einem Dataset fehlerhafte Daten hinzugefügt werden
- **Nichtanerkennung** – Bedrohungen, bei denen es für einen Benutzer möglich ist, eine bestimmte Aktion zu verweigern
- **Offenlegung von Informationen** – Angriffe, bei denen Informationen gegenüber Personen offen gelegt werden, die nicht für den Zugriff autorisiert sind
- **Denial-of-Service** – Angriffe, bei denen gültige Benutzer davon abgehalten werden, auf das System und Systemdaten zuzugreifen
- **Rechteerweiterung** – Bedrohungen, bei denen nicht berechtigte Benutzer ihre Rechte erweitern

Anhand dieser Bewertungen werden geeignete Gegenmaßnahmen in jedes Produkt integriert, um die erkannten Risiken zu minimieren. Mit der Priorisierung dieser Gegenmaßnahmen wird der Schweregrad jedes Risikos entsprechend einer Reihe von Faktoren zur Bewertung der allgemeinen Bedrohung beurteilt:

- **Schadenspotenzial** – Das Potenzial des Schadens steht im Zusammenhang mit der Gesamtmenge der Daten sowie der Auswirkung auf die Vertraulichkeit, Integrität und Verfügbarkeit der Daten.
- **Reproduzierbarkeit** – Die Effektivität eines Angriffs erhöht sich, wenn dieser wiederholt ausgeführt werden kann.
- **Verwertbarkeit** – Ein Angriff kann danach beurteilt werden, wie viel Spezialwissen notwendig ist, um ihn auszuführen.

Durch Bedrohungsmodelle werden Risiken kategorisiert und der Schweregrad bewertet, um eine Priorität zuzuordnen und entsprechende Gegenmaßnahmen einzuleiten.

- **Betroffene Benutzer** – Je mehr Benutzer des Systems von dem Angriff betroffen sind, desto gefährlicher ist dieser Angriff möglicherweise.
- **Aufdeckbarkeit** – Ein Maß für die Verfügbarkeit von Informationen und die Sichtbarkeit von Code, der möglicherweise die Ausführung eines Angriffs unterstützt. Ein wichtiger Beitrag zum Softwareentwurf und Überprüfungsprozess.

Vertrauen schaffen und aufrechterhalten: Das Risikomanagementprogramm von Microsoft Online Services

Dienstsicherheit ist mehr als ein Feature. Es handelt sich um einen kontinuierlichen Einsatz, bei dem erfahrene und qualifiziertes Personal, Software- und Hardwaretechnologien sowie robuste Prozesse zum Entwerfen, Erstellen, Bereitstellen, Betreiben und Unterstützen des Diensts miteinander kombiniert werden. Sicherheit muss sorgfältig verwaltet, regelmäßig verbessert und routinemäßig durch Tests überprüft werden.

Eine effektive, risikobasierte Strategie für Informationssicherheit ist notwendig, um die Vertraulichkeit, Integrität und Verfügbarkeit von Microsoft Online Services und der durch die Dienste verarbeiteten Daten zu schützen.

Bedrohungen der Sicherheit oder Verfügbarkeit des Diensts werden durch den allgemeinen Begriff „Risiko“ beschrieben. Wie wahrscheinlich ist es, dass Ihre Daten intakt und in der gewünschten Anwendung verfügbar sind, wenn Sie sie benötigen? Mit dem Risikomanagementprogramm (RMP) von Microsoft Online Services wird sichergestellt, dass Microsoft Online Services, einschließlich der Business Productivity Online Standard Suite, in einer Weise entwickelt und betrieben werden, die die bewährten Methoden der Branche bezüglich Sicherheit, Datenschutz und Kontinuität übertrifft. Mit dem RMP wird außerdem die fortlaufende Einhaltung dieser Praktiken durch unabhängige Überprüfungen sichergestellt.

Eine ebenso wichtige Priorität des RMP besteht darin, sicherzustellen, dass mit den Onlinediensten in der Business Productivity Online Standard Suite Funktionen und Features bereitgestellt werden, mit denen Kunden die Dienste und ihre eigenen Daten entsprechend ihrer eigenen Richtlinien und Anforderungen verwalten können.

Zielsetzungen des Risikomanagementprogramms

Die Zielsetzungen des Risikomanagementprogramms lassen sich in drei Punkten zusammenfassen:

- **Gewährleisten von Sicherheit und Datenschutz** bei Microsoft Online Services durch Bereitstellung eines effizienten, robusten und ausgereiften Risikomanagementprogramms, das darauf ausgelegt ist, die bewährten Methoden der Branche zu erfüllen bzw. zu übertreffen und, soweit möglich, den behördlichen oder rechtlichen Verpflichtungen des Kunden nachzukommen.
- **Erfüllen der Erwartungen des Kunden** durch die Sicherstellung, dass bei Online Services Features und Funktionen zur Unterstützung geltender Sicherheits- und Kompatibilitätsverpflichtungen zur Verfügung stehen. Dazu wird Fachwissen über Anforderungen vertikaler Märkte und regionaler Bedingungen bereitgestellt und die Transparenz von Sicherheit, Datenschutz und Kontinuität von Online Services gefördert.
- **Kontinuierliches Verbessern und Optimieren** der Online Services-Funktionen durch Produkt- und Dienstinnovationen, Einbringung von Feedback in den Produktveröffentlichungszyklus sowie Bereitstellung von Solution Accelerators zum Erweitern der Anwendbarkeit und Nutzbarkeit von Online Services weltweit.

Erfolgskriterien des Risikomanagementprogramms

Zu den Erfolgskriterien für das Risikomanagementprogramm von Microsoft Online Services zählen:

- **Sichtbarer Support und Einsatz** des Online Services-Managements

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Das Ziel des RMP besteht darin, sicherzustellen, dass Dienste in einer Weise entwickelt und betrieben werden, die die bewährten Methoden der Branche bezüglich Sicherheit, Datenschutz und Kontinuität übertrifft.

- **Die Entwicklung und Umsetzung einer Informationssicherheitsrichtlinie** sowie zugehöriger Zielsetzungen und Aktivitäten, die sich an Geschäftszielen orientieren
- **Weitergabe der Anleitung** für die Informationssicherheitsrichtlinie und zugehörige Standards an alle Mitarbeiter und Vertragspartner
- **Effektive Umsetzung der Sicherheit bei allen Vorgesetzten und Mitarbeitern** sowie eine effektive Weiterbildung und Schulung von Benutzern, um das Personal auf Änderungen der vorhandenen Richtlinie, der unterstützenden Infrastruktur und der Prozesse aufmerksam zu machen
- **Ein umfassendes und ausgewogenes Bewertungssystem**, um die Leistung der Informationssicherheitsverwaltung und Feedback für Verbesserungen auszuwerten

Kerndisziplinen des Risikomanagements

Das Risikomanagementprogramm wurde entwickelt, um geprüfte Praktiken in Bezug auf Entwurf, Entwicklung und Operationen zu gewährleisten, die in der gesamten Microsoft Online Services-Lösung angewendet werden, von der lokal ausgeführten Software, über das Netzwerk, bis hin zur Infrastruktur der Dienste und den Datacentern, in denen sie gehostet werden.

Das Risikomanagementprogramm gliedert sich in vier Bereiche zur Bereitstellung sicherer und verfügbarer Dienste mit erprobter Kompatibilität mit Industriestandards:

- **Sicherheit** – Die Umgebung muss Features zum Schutz vor absichtlichen und unabsichtlichen Angriffen enthalten.
- **Datenschutz** – Daten und Vorgänge eines Kunden müssen vertraulich behandelt und auf diesen Kunden beschränkt werden.
- **Kontinuität** – Die Dienste und zugehörigen Daten müssen bei Bedarf verfügbar sein, und robuste Kapazitäten müssen eine Wiederherstellbarkeit in Katastrophenfällen sicherstellen.
- **Kompatibilität** – Die Dienste müssen in nachweisbarer Kompatibilität mit Microsoft-Sicherheitsrichtlinien und relevanten Industriestandards betrieben werden.

Sicherheit

Dienstsicherheit muss proaktiv in alle Aspekte der Onlinenutzung integriert werden, von der Software selbst bis hin zur unterstützenden Infrastruktur, von den alltäglichen Praktiken Ihrer eigenen Information-Worker bis hin zu den Gebäuden, in denen sich die Datacenter befinden.

Die Sicherheitsarchitektur für Microsoft Online Services richtet sich nach den Schlüsselprinzipien der Trustworthy Computing-Initiative des Unternehmens: Sicherheit durch Design, Standard und Bereitstellung. Das vielseitige Microsoft-Sicherheitsprogramm wurde für globale Unternehmen entwickelt und umfasst einen allgemeinen Satz an Sicherheitsrichtlinien zur Minderung von Risiken und Bedrohungen für Kundendaten. Microsoft verbessert die Sicherheit durch die Standardisierung der Methoden zum Testen, Implementieren und Überwachen der Richtlinien für alle Kunden. Im Gegenzug profitiert jeder Kunde der Business Productivity Online Standard Suite von der Microsoft-Erfahrung mit Sicherheitsbedenken von Kunden weltweit sowie von den von Microsoft angewendeten Praktiken, um diesen Rechnung zu tragen.

Microsoft Online Services sorgen durch Entwurf, Standard und Bereitstellung für Sicherheit.

Ein umfassender, kontinuierlicher Prozess

Bei einer vollständigen Onlinedienstlösung werden Sicherheit und Verfügbarkeit an allen Gliedern der Kette berücksichtigt, von den Benutzern bis zum Personal und den Einrichtungen, von denen die Dienste betrieben werden. Um Angriffe abzuwehren und Kundendaten effektiv zu schützen, wendet Microsoft Online Services das Prinzip des umfassenden Schutzes an, eine Sicherheitsstrategie mit mehreren Ebenen, bei der die verschiedenen Komponenten eines Diensts unabhängig voneinander geschützt werden: die Anwendung, die unterstützende Infrastruktur und Hardware, das Netzwerk sowie die Einrichtung des Datacenters.

Sicherheitsmaßnahmen können im Allgemeinen in zwei Hauptbereiche unterteilt werden:

- **Physische** Sicherheitsmaßnahmen werden für die Gebäude angewendet, in denen sich die gehosteten Dienste, die Computer und andere spezielle Hardware sowie das Betriebspersonal dieser Einrichtungen befinden.
- **Logische** Sicherheitsmaßnahmen werden mittels Software auf den Ebenen des Betriebssystems, der Infrastruktur und der Anwendungen des Systems angewendet.

Physische Sicherheit

Physische Sicherheit wird oft als der kleine Bruder von logischer oder softwarebasierter Sicherheit angesehen. Wenn Kunden sich über Sicherheit und Verfügbarkeit sorgen, denken Sie oft zuerst an Angriffe durch Viren und Malware oder an defekte Festplatten. Die Berücksichtigung der physischen Sicherheit ist jedoch ebenso wichtig, und es ist nicht einfach, sicherzustellen, dass Ihre Daten in Ihren eigenen Einrichtungen sicher sind.

Es muss gewährleistet sein, dass nur autorisiertes Personal Zugang zur Hardware erhält, auf der sich Ihre Geschäftsdaten befinden. Es muss sichergestellt werden, dass Stromausfälle, Personalausfälle oder die physische Verlagerung von Computern nicht den Betrieb beeinträchtigen und die Daten nicht unkalkulierbaren Risiken ausgesetzt werden.

Bei der Migration zu einem Onlinedienst wird diese Verantwortung in einigen Punkten an den Dienstanbieter übertragen. Sie müssen nun darauf vertrauen, dass der Dienstanbieter diese Probleme in Ihrem Namen berücksichtigt und in den Datacentern, in denen sich Ihre Daten befinden, über Lösungen für physische Sicherheitsprobleme verfügt.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

In Datacentern auf der ganzen Welt, die Microsoft Online Services hosten, werden die gleichen strengen physischen und logischen Sicherheitspraktiken angewendet.

Carrier-Class-Datencenter

Microsoft erzwingt physische Sicherheitskontrollen als Teil eines breiten Spektrums an Vorgängen für Carrier-Class-Datencenter. Carrier-Class bedeutet extrem hohe Verfügbarkeit mit lediglich einigen Minuten Ausfallzeit pro Jahr. Die Datencenter, in denen die Dienste der Business Productivity Online Standard Suite betrieben werden, erreichen Carrier-Class-Leistung unter anderem durch folgende Features:

- Physische Gebäudesicherheit
- Sicherer physischer Zugang nur für autorisiertes Personal
- Redundante Stromversorgung:
 - Zwei Hauptstromversorgungen von unterschiedlichen Anbietern
 - Sicherungsakkumulator
 - Dieselgeneratoren (mit alternativen Optionen für Treibstofflieferung)
- Mehrere Faserkabelleitungen zur Verbindung der Datencenter für Redundanz
- Klimatisierung für optimale Temperatur und Luftfeuchtigkeit zum Betrieb der Geräte
- Ggf. seismisch gestützte Racks
- Feuerschutz und Löschsysteme mit minimaler Auswirkung auf die Computerausrüstung
- Bewegungssensoren, 24-stündiger gesicherter Zugang sowie Kameraüberwachung und Sicherheitsalarme

Weltweite Standorte von Datencentern

Die Online Services werden in Datencentern weltweit bereitgestellt, um ein Hosting am geografischen Ort mit globaler Verfügbarkeit anzubieten.

Sicherheit für das Datencenterpersonal

Eine zusätzliche Sicherheitsebene innerhalb des Datencenters wird für das Betriebspersonal angewendet. Der Zugang ist je nach Aufgabenbereich beschränkt, sodass nur die notwendigen Personen autorisiert sind, Anwendungen und Dienste der Kunden zu verwalten. Zur Autorisierung ist Folgendes erforderlich:

- Eingeschränkter Zugang mit Dienstaussweis und Chipkarte
- Biometrische Scanner
- Sicherheitspersonal vor Ort
- Kontinuierliche Videoüberwachung

Zusätzlich muss autorisiertes Personal über eine vorherige Genehmigung für alle Vorgänge und Aktionen innerhalb des Datencenters verfügen. Vorgänge, die nicht bereits Teil von etablierten Prozessen und Prozeduren sind, werden vor ihrer Durchführung überprüft.

Zweistufige Authentifizierung

Datencenter sind „Lights-out“-Bereitstellungen und erfordern Remotesupport und -verwaltung. Der Zugriff für Remotesupport und -verwaltung auf Online Services-Umgebungen erfolgt über einen 128-Bit-verschlüsselten Kommunikationskanal und erfordert eine zweistufige Authentifizierung. Bei der zweistufigen Authentifizierung wird eine physische, vor Fälschungen geschützte Sicherheitsebene mit einem physischen Gerät verwendet. Der Zugriff erfolgt beispielsweise mittels Smartcard und PIN.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Sicherheit bei Entwurf und Vorgängen des Netzwerks

Mehrere separate Netzwerksegmente sorgen für eine physische Trennung der wichtigen Back-End-Server und Speichergeräte von den öffentlich zugänglichen Schnittstellen. Netzwerke innerhalb der Datacenter, in denen Online Services betrieben werden, verfügen über vollständige N+1-Redundanz, und Failoverfeatures helfen, die gesamte Netzwerkausrüstung zu schützen.

Modernste Hardware

Die Server, auf denen die Anwendungen und Dienste ausgeführt werden, sind vollständig redundant mit dualen Netzwerkschnittstellen, dualen Stromversorgungen und vollständiger Lights-out-Verwaltungsfunktion. Die Server werden für maximale Effizienz, Verfügbarkeit und Skalierbarkeit speziell für die Online Services-Architektur konfiguriert. Hardware kann ohne Unterbrechung des Betriebs hinzugefügt oder entfernt werden, und auf die Server kann nur durch autorisiertes Personal über physisch gesicherte Netzwerke mit dedizierten Netzwerkverbindungen zugegriffen werden.

Spezielle Hardware

Microsoft-Datacenter verwenden Hardware, die speziell für die Unterstützung der Software und Dienste von Online Services entworfen und konfiguriert wurde. So wie die Software dafür konzipiert ist, nur die nötigen Funktionen bereitzustellen und die unnötigen zu unterdrücken, ist die Hardware dafür konzipiert, so effizient, effektiv und sicher wie möglich zu arbeiten. Durch diesen Prozess werden die Geschwindigkeit und Effektivität der Konfiguration, Bereitstellung und Sicherung neuer Server erhöht, und es wird sichergestellt, dass die Sicherheitsanforderungen stets eingehalten werden. In diesem Prozess werden außerdem unnötige Kosten sowie unnötiger Strom- und Platzverbrauch eliminiert. Diese Kosteneinsparungen können dann an die Online Services-Kunden weitergegeben werden.

Logische Sicherheit

Logische Sicherheit bei Microsoft Online Services bedeutet Schutz der Software, die bereits auf physisch geschützter Hardware in sicheren Datacentern ausgeführt wird. Der ganzheitliche Microsoft-Ansatz für Softwaresicherheit wird durch sorgfältige Prozesse zur Bewertung und Minderung von Risiken gesteuert.

Features von Microsoft Online Services

Die Anwendungen, aus denen die Online Services bestehen, verfügen über viele Features zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten in der Online Services-Umgebung. Ob in Ihrer Einrichtung oder innerhalb der Online Services-Architektur – diese Features bieten effektive und bewährte Mittel zur Erhöhung der Verfügbarkeit und Verringerung von Risiken.

Sicherheitsfeatures der gehosteten Anwendungen

- **Anmeldungsclient** mit Unterstützung sicherer Benutzerkennwörter, mit der Benutzer auf einfache Weise sicheren Zugang zu mehreren Anwendungen erhalten
- Unterstützung für **authentifizierte und verschlüsselte Kommunikation** zur Identifizierung der Messagingteilnehmer und Verhinderung von Nachrichtenmanipulation
- Unterstützung für Technologien mit **S/MIME (Secure/Multipurpose Internet Mail Extensions) und Rechteverwaltung**, mit denen E-Mails digitale Signaturen und Verschlüsselungstechniken hinzugefügt werden
- **Clientseitige Blockierung von Anlagen** zur Verhinderung potenziell gefährlicher E-Mail-Anlagen
- **Eingeschränktes E-Mail-Relaying** zur Reduzierung von unerwünschten Nachrichten und Spam

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

- **Echtzeit-Sperrlisten** und Listen sicherer Adressen zur Beschränkung von Nachrichten von bekannten Spamquellen
- **Virenfilterung** mit mehreren Ebenen zum Schutz eingehender, ausgehender und interner E-Mails sowie freigegebener Dateien Ihrer Organisation
- **Flexible Geräterichtlinien** zum Schutz mobiler Gerätekommunikation (wie z. B. PIN-Sperrung und ferngesteuerte oder lokale Zurücksetzung)

Die Infrastruktur von Microsoft Online Services

Die Infrastruktur von Online Services besteht aus der Hardware, der Software und den Netzwerken, die für die Ausführung der Online Services in den physischen Einrichtungen der Datacenter erforderlich sind.

Die Sicherheitsmaßnahmen innerhalb der Dienstinfrastruktur sind wahrscheinlich strenger als die, die ein Unternehmen in einem eigenen Netzwerk umsetzen könnte. Zu den Sicherheitsmaßnahmen auf Infrastrukturebene zählen:

- **Sicherheitsoptimierte Benutzeroberflächen**, auf denen die verfügbaren Features so gefiltert werden, dass der jeweilige Benutzer nur auf die für ihn autorisierten Aktionen, Links und Inhalte zugreifen kann
- **Umfassender Support für Serverüberwachung**, der in die gesamte dienstweite Microsoft System Center Operations Manager-Überwachungsarchitektur integriert ist
- **Sicherer Remotezugriff** über Windows Server® 2008-Terminaldienste
- **Verwaltung in mehreren Ebenen** unter Verwendung eines Verwaltungsmodells mit drei Ebenen, bei dem Verwaltungsaufgaben isoliert werden. Der Zugriff darauf wird entsprechend der Benutzerrolle und der Ebene des Verwaltungszugriffs gesteuert, für die der Benutzer autorisiert ist.
- **Antivirusscanning auf Serverebene** zum Schutz vor Viren, die das Serverbetriebssystem angreifen
- **Sicherheitsüberprüfung der Umgebung** zum Überwachen von Schwachstellen und fehlerhafter Konfiguration
- **Angriffserkennungssysteme** zur Überwachung aller Zugriffe auf Online Services rund um die Uhr. Diese Daten werden von ausgereiften Korrelationsmodulen analysiert, um das Personal sofort über verdächtige Verbindungsversuche zu informieren.

Bei Microsoft Online Services wird umfassender Schutz praktiziert. Mit der Sicherheitsstrategie in mehreren Ebenen werden die Komponenten eines Netzwerks mithilfe verschiedener Mechanismen, Prozeduren und Richtlinien geschützt.

Sicherheitsstandards der Betriebssysteme

Um Online Services vor Angriffen durch böswillige Benutzer oder schädlichen Code zu schützen, werden beim Betriebssystem besondere Vorkehrungen getroffen. Die Absicherung des Betriebssystems umfasst das Deaktivieren nicht benötigter Dienste, das Sichern von Dateifreigaben mittels Autorisierungsanforderung sowie das Implementieren des Features zur Datenausführungsverhinderung. Bei der Datenausführungsverhinderung handelt es sich um einen Satz von Hardware- und Softwaretechnologien, mit denen zusätzliche Überprüfungen am Speicher vorgenommen werden, um die Ausführung von schädlichem Code zu verhindern.

Alle Server innerhalb der Online Services-Umgebung werden regelmäßig mit Sicherheitsupdates für die verwendete Software aktualisiert. Der Zeitpunkt für das Anwenden von Updates richtet sich jeweils nach Gefährlichkeit, Umfang und Auswirkung der entsprechenden Sicherheitslücke.

Systemverwaltung und Zugriffssteuerung

Die Verwaltung der Netzwerke und Komponentenserver, auf denen die Online Services ausgeführt werden, wird durch den Active Directory®-Dienst bereitgestellt. Anwendungen, die die Online Services bereitstellen, wurden für die effiziente und effektive Ausführung innerhalb der Active Directory-Umgebung entwickelt.

Das Personal verwaltet und erzwingt die Sicherheitsrichtlinien zentral von gesicherten Servern aus, die für die Steuerung und Überwachung netzwerkweiter Systeme dediziert sind. Durch ein delegiertes Verwaltungsmodell erhalten Administratoren nur Zugriff für die

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Durchführung bestimmter Aufgaben. Dadurch wird das Fehlerpotenzial reduziert und der Zugriff auf Systeme und Funktionen nur nach Bedarf gewährt.

Neue Server können schnell und sicher konfiguriert werden, und mit einer vorlagenbasierten Serverabsicherung wird gewährleistet, dass neue Kapazitäten mit bereits implementierten Sicherheitsmaßnahmen online gestellt werden.

Das Netzwerk von Microsoft Online Services

Netzwerkverbindungen von Ihrem Unternehmen zu den Online Services werden mit dem SSL (Secure Sockets Layer)-Protokoll durch Zertifikate geschützt.

Die Kommunikation ist durch 128-Bit-Verschlüsselung geschützt. Microsoft versucht, sicherzustellen, dass nicht nur die in den Online Services gespeicherten Daten geschützt sind, sondern dass auch alle Datenübertragungen während der Verwendung der Online Services geschützt sind.

Die bei der Online Services-Plattform eingehenden Verbindungen werden anhand strenger Sicherheitsrichtlinien geprüft, bevor sie durch Filter und Firewalls in das Netzwerk gelangen können. Vollständige N+1-Redundanz im gesamten Netzwerk sorgt für eine komplette Failover-Funktion sowie für eine 99,9-prozentige Verfügbarkeit des Netzwerks.

Firewalls und Filterrouter

Firewalls und Filterrouter an der Grenze des Online Services-Netzwerks sorgen für eine gut eingerichtete Sicherheit auf Paketebene, um nicht autorisierte Verbindungsversuche zu verhindern. Dadurch wird sichergestellt, dass die tatsächlichen Inhalte der Pakete Daten im erwarteten Format enthalten und dem erwarteten Client-/Server-Kommunikationsschema entsprechen. Firewalls schränken außerdem die Datenkommunikation auf bekannte und autorisierte Ports, Protokolle und Ziel-IP-Adressen ein. Auf diese Weise wird der Zugang zu den Online Services auf die Ports und Protokolle beschränkt, die für die Kommunikation zwischen den Online Services und den Online Services-Kunden erforderlich sind.

Schutz vor bössartiger Software

Die Dienste der Business Productivity Online Standard Suite führen mehrere Ebenen von Antivirussoftware aus, um Schutz vor bekannter bössartiger Software zu gewährleisten. Beispielsweise wird auf allen Servern innerhalb der Business Productivity Online Standard Suite-Umgebung Antivirussoftware ausgeführt, die das Betriebssystem auf Viren überprüft. Darüber hinaus wird auf Microsoft Exchange Server-Mailservern zusätzliche Antivirussoftware ausgeführt, die speziell E-Mails auf potenzielle Gefahren überprüft.

Durch diese Maßnahmen werden auch Viren abgewehrt, die möglicherweise unbeabsichtigt mit den Daten Ihrer Benutzer eingeführt wurden.

Operations von Weltklasse

Operations ist eine Schlüsselkomponente für die allgemeine Sicherheit und Verfügbarkeit der Microsoft Online Services. Dabei handelt es sich um eine der Kernkompetenzen, auf die Unternehmen bei ihren Onlinediensteanbietern achten. Einen bedeutenden Teil der Ausgaben für den Betrieb Ihrer eigenen Software vor Ort stellen Verwaltung und Wartung dar, für die entsprechendes Supportpersonal erforderlich ist. Ein wichtiger Wert bei der Verwendung von Microsoft Online Services ist das bewährte Fachwissen des Microsoft Online Services-Operations-Teams.

Bei der Verwaltung von Änderungen, Störungen und Problemen folgt das Microsoft-Personal den Industriestandards der Information Technology Infrastructure Library (ITIL). ITIL stellt ein Framework von Richtlinien und bewährten Methoden für das Verwalten von Softwarediensten und -infrastrukturen bereit. Diesem Satz an Anforderungen hat Microsoft ein eigenes Microsoft Operations Framework (MOF) hinzugefügt, ein vorgeschriebener Satz von Prozeduren zur standardisierten Implementierung von ITIL-Empfehlungen. MOF stellt einen integrierten Satz an bewährten Methoden, Prinzipien und Aktivitäten bereit, mit dem Organisationen die Zuverlässigkeit ihrer IT-Lösungen und -Dienste gewährleisten können.

MOF definiert und standardisiert Prozeduren für ein termingerechtes und risikoarmes Änderungsmanagement. Darüber hinaus wird die Definition eines Pfads für die Problemverwaltung vom Kunden über Operations bis hin zu Produktentwicklungsteams unterstützt.



Microsoft Online Services verwendet das Microsoft Operations Framework für Dienstbereitstellung und Operations

Überwachung und Risikominderung

Um Risiken proaktiv zu minimieren und die Verfügbarkeit von Anwendungen und Daten sicherzustellen, investiert Online Services in Tools und Dienste zur Überwachung.

Microsoft System Center Operations Manager

Server innerhalb der Online Services-Umgebung werden für die Maximierung der Sicherheitereignisse von Betriebssystem und Anwendungen konfiguriert. Dadurch entsteht ein umfangreicher Überwachungspfad der Verwendung von Anwendungen, und etwaige Sicherheitsausnahmen werden protokolliert. Das Online Services-Operations-Team nutzt die neueste Technologie und optimierte Prozesse, um eingehende Informationen zu sammeln, zu korrelieren und zu analysieren.

Die Online Services-Hostumgebung verwendet Microsoft System Center Operations Manager, eine End-to-End-Dienstverwaltungsumgebung, die in die Plattform, Diensthardware und -software integriert ist, um eine Zustandsüberwachung rund um die Uhr zu gewährleisten.

Spezielle Management Packs werden über die Online Services-Plattform geschichtet, um das Betriebspersonal mit sehr spezifischen Informationen zu versorgen, mit denen Trends erkannt und Verhaltensweisen vorhergesagt werden können, die eventuell einen proaktiven Eingriff erfordern. Die Management Packs von System Center Operations Manager bieten eine interne Transaktionsüberwachung, Funktionen für das Überprüfen von Schwellenwertmodellen für Dienste sowie eine Analyse der CPU-Nutzung, die auf die Online Services-Anwendungen zugeschnitten ist.

Integrierte Überwachung der Infrastruktur- und Internetleistung

Die von System Center Operations Manager bereitgestellten Daten werden kombiniert mit Eingaben aus zusätzlichen spezialisierten Tools und Diensten zum Erfassen, Aggregieren und Analysieren des Netzwerks der Online Services sowie des Verhaltens von Schlüsselwebsites im Internet. Wenn sich beispielsweise die Konnektivität verschlechtert, kann das Personal ermitteln, ob ein internes Problem bei einem der Online Services vorliegt oder ob Bedingungen im Internet dafür verantwortlich sind, die möglicherweise ein Risiko für Kunden der Business Productivity Online Standard Suite darstellen.

Überwachung von Hardware- und Softwaresubsystemen

Bei der proaktiven Überwachung wird die Leistung wichtiger Subsysteme der Online Services-Plattform kontinuierlich gemessen. Für die Online Services wurden Schwellenwerte festgelegt, die die Grenzen für akzeptable Dienstleistung und -verfügbarkeit darstellen. Wenn ein Schwellenwert erreicht wird oder ein anomales Ereignis eintritt, werden vom Überwachungssystem Warnungen generiert, sodass das Betriebspersonal reagieren kann. Zu den Beispielen für bestimmte Schwellenwerte zählen:

- **CPU-Nutzung** – Ein nicht kritischer Warnschwellenwert ist bei 80 Prozent Auslastung festgelegt. Ein kritischer Warnschwellenwert ist bei 90 Prozent festgelegt.
- **Dienstnutzung** – Verschiedene Dienstkomponenten wie Dienstlizenzen, Kapazität für E-Mails und Microsoft SharePoint Online werden alle überwacht.
- **Speicherauslastung** – Wenn sich die Speicherreserven auf 15 Prozent verringern, wird eine nicht kritische Warnung angezeigt. Wenn die Speicherreserven 7 Prozent erreichen, wird eine kritische Warnung angezeigt.
- **Netzwerklatenz** – Nicht kritische Warnungen werden angezeigt, wenn die Netzwerklatenz bei 100 Millisekunden liegt, und eine kritische Warnung wird bei 300 Millisekunden ausgegeben.

Protokollierung von Ereignissen und Aktivitäten

Überwachung ist eine Schlüsselkomponente der Sicherheitsstrategie von Online Services. Sicherheitsüberwachung bietet zwei Hauptvorteile für die Business Productivity Online

Microsoft

Online Services Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Das Personal überwacht sowohl die interne Leistung von Netzwerk und Diensten als auch die externen Internetbedingungen, die die Nutzung von Microsoft Online Services beeinträchtigen könnten.

Standard Suite: die Möglichkeit, Angriffe zu erkennen, sobald sie auftreten, und die Möglichkeit, forensische Analysen der Ereignisse durchzuführen, die vor, während und nach einem Angriff aufgetreten sind.

Durch das sofortige Erkennen von Angriffen kann das Microsoft-Personal schnell reagieren, um substanziellen Schaden an den Diensten und der Infrastruktur abzuwehren. Durch die forensischen Daten können Ermittler außerdem das Ausmaß des Angriffs bestimmen.

Die Protokollierung von Zugriffen und Aktivitäten ist ein wichtiger Aspekt der Sicherheit. Die Überwachung der Erstellung und Änderung von Objekten bietet eine Möglichkeit, potenzielle Sicherheitsprobleme nachzuverfolgen, die Verantwortlichkeit von Benutzern sicherzustellen sowie im Fall einer Sicherheitsverletzung Indizien zu liefern. Das Online Services-Operations-Programm überwacht und protokolliert Informationen zu den folgenden Ereignistypen:

- Kontoanmeldeereignisse
- Kontoverwaltung
- Verzeichnisdienstzugriff
- Anmeldeereignisse
- Objektzugriff
- Richtlinienänderungen
- Rechtenutzung
- Prozessnachverfolgung
- Systemereignisse

Microsoft führt kontinuierlich eine interne und externe Schwachstellenbewertung der Microsoft Online Services-Netzwerke durch.

Integration von Sicherheit und Operations

Microsoft Online Services verfügt über eine dedizierte Sicherheitsorganisation, die auf konstante Sicherheitsüberwachung ausgerichtet ist, mit Personal, das den im MOF definierten Prinzipien folgt. Aus breiterer Sicht des Betriebs strukturiert Microsoft interne Vorgänge basierend auf dem ITIL (Information Technology Infrastructure Library)-Framework. Das Sicherheitsteam folgt den in ITIL definierten Funktionen und wendet diese auf die Vorgänge der Online Services an:

1. **Änderungsmanagement** – Änderungsmanagement ist ein wichtiges Element, um sicherzustellen, dass Ihre Daten geschützt und jederzeit verfügbar sind. Das Team der Business Productivity Online Standard Suite folgt den ITIL-Richtlinien zum Änderungsmanagement für einen regulierten Ansatz zur Änderung der Umgebung. Microsoft hält mit der zunehmenden Popularität des Software-plus-Services-Modells Schritt. Dazu werden Netzwerke, Serverkapazität und Softwarefunktionen hinzugefügt. Jede Änderung innerhalb der Umgebung wird durch das Microsoft Online Services-Sicherheitsteam auf die Möglichkeit geprüft, ob dadurch Ausfallzeiten oder unbeabsichtigte Konsequenzen entstehen könnten.
 - **Störungsmanagement** – Die Online Services-Operations-Gruppe empfängt Warnungen aus einer Vielzahl von Quellen. Zu diesen Quellen zählen E-Mails von Kunden, Telefonanrufe sowie System- und Sicherheitsüberwachungstools. Jede Warnung wird untersucht, um zu entscheiden, ob eine Störung vorliegt. In einigen Fällen kann eine Warnung als Sicherheitsvorfall klassifiziert und durch interne Microsoft-Supportgruppen entsprechend eskaliert werden. Wenn die Störung die Sicherheit beeinträchtigt, arbeitet das Sicherheitspersonal von Microsoft Online Services mit Produktexperten zusammen, um eine schnelle Untersuchung, Reaktion und Behebung der Störung sicherzustellen.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

- **Problemverwaltung** – Wenn eine Störung regelmäßig auftritt, ist die geeignete Reaktion möglicherweise eine Änderung der Dienstkonfiguration oder eine Empfehlung an eine Microsoft-Produktgruppe, ein neues Feature einzuführen. Das Sicherheitspersonal von Microsoft Online Services unterstützt die Definition und Überprüfung der entsprechenden Dienst- oder Produktänderung.

Aufgabentrennung für Personal

Microsoft Online Services erfordert separates Personal für die Entwicklung, Bereitstellung und den Betrieb der gehosteten Dienste, um das Prinzip der Aufgabentrennung einzuhalten. Dies umfasst die Kontrolle des Zugriffs auf den Quellcode, die Build-Server sowie die Produktionsumgebung.

Der Zugriff auf die Produktionsumgebung der Business Productivity Online Standard Suite ist auf das Betriebspersonal beschränkt. Entwicklungs- und Testteams erhalten möglicherweise temporären Zugriff, um Probleme zu beheben. Dieser Zugriff wird jedoch nur im Einzelfall nach Bedarf gewährt.

Der Zugriff auf den Quellcode der Online Services ist beschränkt auf das Entwicklungspersonal. Das Betriebspersonal kann den Quellcode nicht ändern.

Umsetzung der Prinzipien des Risikomanagements

Die Betriebsstrategie umfasst den folgenden Satz an Risikomanagementprinzipien, um Risiken bei der Dienstbereitstellung zu minimieren:

- **Umfassender Schutz** – Allgemeine Sicherheit lässt sich nicht durch einen einzelnen Verteidigungsmechanismus erreichen. Auf jeder Ebene der Business Productivity Online Standard Suite-Infrastruktur, vom Umfang des Netzwerks bis zu den Servern und Diensten mit den Kundendaten, aus denen die Infrastruktur besteht, sind Kontrollen zur Abwehr von Angriffen implementiert.
- **Identitätsverwaltung** – Effektive Zugriffssteuerungen basieren auf einer ordnungsgemäßen Identitätsverwaltung und rollenbasierter Autorisierung.
- **Bereichsbildung** – Die Systeme für Kunden, Anwendungen, Dienste und Verwaltung von Online Services befinden sich in getrennten Sicherheitszonen. Zugriff und Kommunikation zwischen den Systemen in verschiedenen Zonen werden sorgfältig verwaltet, um Datenverlust zu verhindern und um Eindringlingen in einer Zone den Angriff von Systemen in anderen Zonen zu erschweren.
- **Redundanz** – Online Services verfügt über redundante Server, Netzwerkkomponenten sowie geografisch verteilte Einrichtungen, um die Verfügbarkeit sicherzustellen.
- **Einfachheit** – Bereitstellungen der Business Productivity Online Standard Suite sind für Einfachheit optimiert. Je komplexer Systeme sind, desto schwieriger sind sie zu schützen. Durch Einfachheit wird die Wahrscheinlichkeit von Konfigurations- oder Betriebsfehlern verringert.
- **Mindestberechtigung** – Benutzern und Systemen wird nur der minimal erforderliche Zugriff zur Durchführung der vorgegebenen Aufgaben gewährt.
- **Verantwortlichkeit** – Die Aktionen von Personen innerhalb der Business Productivity Online Standard Suite-Umgebung sind bis hin zu Einzelbenutzern oder Personal nachverfolgbar.
- **Überwachung** – Die Systeme umfassen Überwachungsmechanismen, um nicht autorisierte Nutzung zu erkennen und die Untersuchung von Störungen zu unterstützen.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

- **Sicherer Status bei Fehlern** – Die Systeme sind so angelegt, dass die Effektivität aktueller Sicherheitskontrollen durch Systemfehler nicht beeinträchtigt wird.
- **Operational Excellence** – Microsoft verfügt über geschultes Betriebspersonal und klar definierte Prozeduren, um die Online Services-Systeme zu verwalten und auf Ausfälle und Störungen zu reagieren.
- **Universelle Mitwirkung** – Eine starke Sicherheitsinfrastruktur erfordert die Zusammenarbeit aller Parteien in der Umgebung. Angriffe können von überall stammen. Daher müssen Personal, Partner, Anbieter und Kunden von Microsoft Online Services aktiv am Sicherheitsprogramm teilnehmen.

Verwaltung von Sicherheitsvorfällen

Sicherheitsvorfälle sind in der Online Services-Umgebung selten. Microsoft hat jedoch widerstandsfähige Prozesse entwickelt, um eine koordinierte Reaktion auf Vorfälle zu ermöglichen, sobald diese auftreten.

Zu Sicherheitsvorfällen zählen unter anderem E-Mail-Viren, Rootkits, Würmer, Denial-of-Service-Angriffe, nicht autorisierter Zugriff, unsachgemäße Nutzung von Netzwerkressourcen sowie andere Arten von nicht autorisierten, unzulässigen oder ungesetzlichen Aktivitäten bezüglich der Online Services-basierend auf Computernetzwerken oder Datenverarbeitungseinrichtungen.

Der Online Services-Prozess zur Reaktion auf Sicherheitsvorfälle umfasst die folgenden Phasen:

- **Identifizierung** – System- und Sicherheitswarnungen werden erfasst, miteinander in Beziehung gesetzt und analysiert. Ereignisse werden von den Betriebs- und Sicherheitsteams von Microsoft untersucht. Wenn ein Ereignis auf ein Sicherheitsproblem hindeutet, wird dem Vorfall ein Schweregrad zugeordnet, um ihn innerhalb von Microsoft angemessen zu eskalieren. Diese Eskalation umfasst Produkt-, Sicherheits- und Entwicklungsspezialisten.
- **Eindämmung** – Das Eskalationsteam bewertet Umfang und Auswirkung des Vorfalls. Die unmittelbare Priorität des Eskalationsteams besteht darin, sicherzustellen, dass der Vorfall eingedämmt und Daten geschützt werden. Das Eskalationsteam bestimmt eine Reaktion, führt entsprechende Tests durch und implementiert die Änderungen. In Fällen, bei denen eine tiefer gehende Untersuchung erforderlich ist, werden modernste forensische Software und bewährte Methoden der Branche eingesetzt, um Informationen aus den betroffenen Systemen zu erfassen.
- **Abarbeitung** – Nach der Eindämmung des Vorfalls fährt das Eskalationsteam mit der Abarbeitung des durch die Sicherheitsverletzung entstandenen Schadens fort und ermittelt die Ursache des Sicherheitsproblems. Wenn eine Schwachstelle gefunden wird, meldet das Eskalationsteam das Problem an die Produktentwicklung.
- **Wiederherstellung** – Bei der Wiederherstellung werden Software- oder Konfigurationsupdates auf das System angewendet, und die Leistungskapazität der Dienste wird wieder vollständig hergestellt.
- **Gelernte Lektionen** – Jeder Sicherheitsvorfall wird analysiert, um sicherzustellen, dass angemessene Gegenmaßnahmen getroffen werden, um zukünftige Wiederholungen zu vermeiden.

Sicherheitsuntersuchung

Bei bedeutenden Sicherheitsereignissen startet das Personal von Microsoft Online Services umfassende Untersuchungen, um die Hintergründe des Vorfalls zu klären und eine abschließende Beschreibung dafür zu finden.

Bei einigen Vorfällen ist eine forensische Untersuchung erforderlich. Eine forensische Untersuchung umfasst das sorgfältige Sammeln und Analysieren von Indizien für einen Sicherheitsvorfall. Der Prozess umfasst das Nachstellen eines Vorfalls in einer rekonstruierten Umgebung, um die verschiedenen Theorien zu belegen oder zu widerlegen, die sich aus der Untersuchung ergeben. In einigen Fällen stützt sich das Online Services-Sicherheitspersonal bei der Analyse auf die umfangreiche Erfahrung anderer Microsoft-Teams.

Das Online Services-Sicherheitsteam unterstützt auch Kunden bei Sicherheitsangelegenheiten, die sie nicht selbst mit den zur Verfügung stehenden Protokollen und Tools der Online Services-Plattform untersuchen können. Diese Aktivität wird im

Microsoft

Einzelfall durchgeführt, je nach Situation und Umfang des Bedarfs an Online Services-Ressourcen.

Datenschutz bei Microsoft Online Services

Microsoft hat erkannt, dass Datenschutz ein grundlegendes Element einer sicheren Computernutzung ist. Kunden haben hohe Erwartungen bezüglich der Erfassung, Nutzung und Speicherung ihrer Daten durch Microsoft. Datenschutz ist neben Sicherheit, Zuverlässigkeit und geschäftlicher Integrität einer der vier Grundpfeiler der Microsoft Trustworthy Computing-Initiative. Microsoft setzt umfangreiche Ressourcen zur Verbesserung des Datenschutzes ein. Dadurch wurde Datenschutz als selbstverständliche Priorität in der Kultur aller Unternehmensbereiche von Microsoft verankert.

Datenschutz schon beim Entwurf

Die Anstrengungen für Datenschutz konzentrieren sich auf drei Schlüsselbereiche: Technologie, Partnerschaft und Zusammenarbeit sowie Kundenanleitung und -engagement. Durch Richtlinien und Prozesse stellt Microsoft Folgendes sicher:

- Integration von Datenschutz in die Produkte während des gesamten Produktlebenszyklus
- Implementieren von datenschutzbasierter Technologie bei allen internen Prozessen
- Ordnungsgemäße Umsetzung globaler Datenschutzpraktiken im gesamten Unternehmen
- Führungsrolle in der Branche

Schutz von Kundendaten unabhängig vom Wohn- oder Arbeitsort

Um eine vertrauliche Umgebung für Kunden zu schaffen, berücksichtigt Microsoft bei der Entwicklung von Software, Diensten und Prozessen stets den Datenschutz. Microsoft geht bei der Einhaltung globaler Datenschutzgesetze sorgfältig vor. Die Datenschutzpraktiken sind teilweise von weltweiten Datenschutzgesetzen abgeleitet. Microsoft folgt der Essenz dieser Datenschutzgesetze und wendet diese Standards global an.

Zusätzlich trifft Microsoft technische und organisatorische Sicherheitsmaßnahmen, um einen ordnungsgemäßen Umgang mit Kundendaten sicherzustellen.

Spezielle Datenschutzpraktiken: Marketing und Werbung sowie Tests

Zwei Bereiche von Microsoft-Praktiken beim Umgang mit Informationen sind für Kunden von besonderem Interesse: Marketing und Werbung sowie Tests.

Marketing und Werbung

Microsoft-Vermarktung findet nur gegenüber dem Geschäftskunden statt, der den Dienst registriert und erworben hat (oder gegenüber einem Nachfolger als designierter Kontakt und Stellvertreter des Kunden). Microsoft wendet sich nicht an Benutzer des Kunden und verwendet keine persönlichen für die Bereitstellung des Diensts erfassten Informationen für Marketing- oder Werbezwecke, außer mit dem ausdrücklichen Einverständnis des Kunden.

Tests

Zur Verbesserung der Online Services stellt Microsoft möglicherweise einen Beispielsatz an Daten aus den Online Services automatisch zusammen, um damit Server vor geplanten Updates zu testen. Dadurch wird sichergestellt, dass Probleme frühzeitig erkannt werden, dass der Dienst nicht unterbrochen wird und dass in Zukunft weniger Supportvorfälle auftreten.

Wenn Microsoft darüber hinaus Spam oder Malware identifiziert, die aus Ihrem Konto stammt, können diese Informationen isoliert werden, um die Sicherheit des Microsoft-Netzwerks für alle Benutzer zu verbessern.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Anbieter und Partner

Um die Bereitstellung der Dienste zu unterstützen, werden gelegentlich Informationen an andere Unternehmen weitergegeben, die in begrenztem Umfang Dienste im Auftrag von Microsoft ausführen. Von den Firmen wird verlangt, dass sie die Vertraulichkeit persönlicher Informationen wahren, und ihnen wird untersagt, die Informationen zu irgendeinem anderen Zweck zu nutzen.

Anbieter

Alle Microsoft-Anbieter müssen dem Microsoft Vendor Privacy Assurance Programm beitreten, das sie zur Einhaltung der Microsoft-Standards für Datenschutz verpflichtet. Microsoft erzwingt die Befolgung des Anbieters durch Verträge und Überprüfungen.

Partner

Wenn ein Kunde Features oder Support von Microsoft-Partnern anfordert, gibt Microsoft persönliche Informationen an diese Partner in Bezug auf diese Anforderung weiter. Microsoft ist nicht für die Handhabung der Privatsphäre und des Datenschutzes auf Seiten der Partner verantwortlich. Microsoft teilt jedoch immer klar mit, dass persönliche Informationen weitergegeben werden, wenn ein Kunde sich für die Verknüpfung seines Kontos mit einem Microsoft-Partner registriert. Darüber hinaus kann ein Kunde sich entscheiden, zu keinem Zeitpunkt Informationen an Partner herauszugeben. Die Weitergabe von Informationen wird ab diesem Moment unterbunden.

Zugriff, Sicherheit, Datenintegrität und Erzwingung

Um sicherzustellen, dass Kunden die Kontrolle über ihre eigenen Daten behalten, bieten die Microsoft Online Services dem Administrator oder Stellvertreter des Kunden vollen Zugriff auf die Kundenumgebung, einschließlich Postfächern und Websites der Benutzer, sodass die eigenen Sicherheits- und Datenschutzrichtlinien des Unternehmens erzwungen werden können.

Entweder auf Anforderung oder auf regelmäßiger Basis stellt Microsoft Datensätze mit Einzelheiten zu Administratorzugriffen auf Postfächer von Benutzern bereit, sodass Kunden ihre Richtlinien bezüglich angemessener Verhaltensweisen für ihre Dienstadministratoren überprüfen und erzwingen können. Diese Datensätze enthalten auch den Zugriff durch Supportpartner und das Microsoft-Supportpersonal, außer wenn dies aufgrund eines rechtlichen Verfahrens untersagt ist.

Kundenanleitung

Sicherheit und Datenschutz beginnt in Ihren Einrichtungen. Daher enthalten die Dienste der Business Productivity Online Standard Suite Dokumentation, Anwendungen und Dienstprogramme, die es für Benutzer und Administratoren einfach machen, Microsoft bei der sicheren und vertraulichen Aufbewahrung Ihrer Daten zu unterstützen.

Onlineweboberflächen oder -portale bieten eine einfache und direkte Anleitung für Benutzer und Administratoren. Administratoren können Benutzer und Dienste bereitstellen sowie die Nutzung von Diensten der Business Productivity Online Standard Suite innerhalb ihrer Organisation überwachen. Benutzer können die ihnen zugewiesenen Dienste aufrufen und verwalten. Mit einer Anwendung für einmaliges Anmelden können auf einfache und bequeme Weise sichere Kennwörter erstellt und verwendet werden. Das Ziel ist eine von Grund auf sichere und vertrauliche Onlinenutzung, da Schutzmaßnahmen am effektivsten sind, wenn sie transparent und leicht zu befolgen sind.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Als Kunde der Business Productivity Online Standard Suite tragen Sie die Verantwortung dafür, mit der Anpassung des Featuresatzes an Ihre Bedürfnisse Richtlinien, Praktiken und Bestimmungen einzuhalten. Beispielsweise sollten Sie relevante Datenschutzgesetze und -bestimmungen auswerten, Mitarbeiter und andere Benutzer über Speicherort und Verarbeitung der Daten informieren und deren Einwilligung einholen sowie ein entsprechendes Maß an Schutz für verschiedene Klassen persönlicher Informationen in Ihrer Organisation definieren.

Innerhalb der Online Services werden persönliche Informationen mit Einwilligung des Kunden oder anwendbaren Gesetzen entsprechend erfasst, verarbeitet und übertragen. Ihre persönlichen Informationen werden ausschließlich für Bereitstellung, Betrieb und Verbesserung von Microsoft-Produkten und -Diensten verwendet.

Das Whitepaper [Privacy and Trust in a Connected World](#) (in englischer Sprache) bietet weitere Informationen darüber, wie Microsoft Kunden dabei unterstützt, Datenschutz für Einzelpersonen und Organisationen durch eine Kombination von Technologieinnovation und -investitionen, Führung und Zusammenarbeit sowie Kundenanleitung und -engagement zu verbessern.

Internationale Datenübertragung

Ein Ziel von Microsoft Online Services ist es, für Benutzer in so vielen Absatzgebieten wie möglich verfügbar zu sein.

Informationen, die von Microsoft erfasst oder an Microsoft gesendet wurden, werden möglicherweise in den Vereinigten Staaten oder in anderen Ländern/Regionen gespeichert und verarbeitet, in denen Microsoft oder dessen Partnerunternehmen, Niederlassungen oder Dienstanbieter Einrichtungen haben.

Für Kunden in der Europäischen Union ist Microsoft vom US-Handelsministerium Safe Harbor-zertifiziert. Microsoft richtet sich nach den Safe Harbor-Bestimmungen bezüglich der Erfassung, Verwendung und Aufbewahrung von Daten aus der Europäischen Union. Dadurch wird die legale Übertragung von Daten sichergestellt, die aus der Europäischen Union und anderen Ländern, die ihre Datenschutzgesetze an die Europäische Union angepasst haben, zur Verarbeitung an Microsoft gesendet werden.

Verwaltung der Dienstkontinuität

Daten können versehentlich oder mit böswilliger Absicht gelöscht werden. Die Verwaltung von Sicherheit und Verfügbarkeit ist eng miteinander verwoben, um Dienste und Daten zu erstellen, die stets verfügbar sind, wenn Sie sie benötigen. Die Verwaltung der Dienstkontinuität sorgt jedoch für die zusätzliche Fähigkeit, Ausfälle und Datenverluste proaktiv zu vermeiden und Wiederherstellungen durchzuführen, wenn solche Notfälle auftreten.

Viele Generationen von Software für Diensthosp Plattformen und Hardwaredesign sowie Bereitstellungs- und Schulungserfahrung werden nun in der Business Productivity Online Standard Suite umgesetzt. Diese in der Branche führende Erfahrung wird an allen Punkten bei Entwurf, Bereitstellung, Betrieb und Support von Microsoft Online Services angewendet, um Ihr Geschäft vor Ausfallzeiten wegen nicht verfügbarer Daten oder Datenverlust zu schützen.

Messagingkontinuität durch Archivierung

Der Zugriff auf den E-Mail-Dienst und auf zurückliegende E-Mail-Vorgänge ist sowohl für die Geschäftskontinuität als auch zur Erfüllung von rechtlichen Vorschriften wichtig.

Die Business Productivity Online Standard Suite verfügt über eine gehostete Archivoption, die fortschrittliche Nachrichtenarchivierung und Kompatibilitätstools für E-Mails, Sofortnachrichten und Bloomberg-Nachrichten bietet. Das gehostete Archiv verfügt über die folgenden Features:

- **Bequemer Zugriff:** Als Tool für die Geschäftskontinuität können E-Mail-Administratoren und Endbenutzer auf das Archiv zugreifen, um Nachrichten wiederherzustellen, die in der primären E-Mail-Umgebung möglicherweise verloren gegangen sind oder gelöscht wurden.
- **Kontinuierlicher E-Mail-Empfang:** Wenn der normale E-Mail-Empfang durch einen Ausfall der primären E-Mail-Umgebung oder des Unternehmensnetzwerks blockiert ist, werden Nachrichten weiterhin in das gehostete Archiv kopiert. Die ursprünglichen Nachrichten werden in eine Warteschlange gestellt und später zugestellt, sobald die primäre E-Mail-Umgebung wieder verfügbar ist.
- **Vollindizierte Datenbank:** Beim Archivieren von Nachrichten werden diese samt Metadaten, Nachrichtentext und den in der Datenbank gespeicherten Anlagen volltextindiziert. Alle Datenbankserver verfügen über vollständig funktionsfähige Standbydatenbanken, die separat gesichert werden. Transaktionsprotokolle werden regelmäßig über das SSH (Secure Shell)-Protokoll aus jeder primären Datenbank an die entsprechende sekundäre Datenbank übermittelt, und die Redundanz der archivierten Daten eines Kunden wird mit einem regelmäßigen Sicherungsplan gewährleistet.

Datenspeicher

Spezialisierte Speicherserver sorgen für eine redundante, gespiegelte Speicherung der Kundendaten. Durch eine kontinuierliche Offsite-Spiegelung zwischen Datacentern verschiedener geografischer Orte wird sichergestellt, dass die Daten selbst im unwahrscheinlichen Fall eines vollständigen örtlichen Datacenterausfalls sicher und aktuell sind. Alle Daten werden auf Festplatten anstatt auf Band gespeichert, um eine schnelle, fehlerfreie Wiederherstellung zu ermöglichen, auf Clusterservern mit von Microsoft System Center Data Protection Manager bereitgestellten Sicherheitsdiensten. Data Protection Manager bietet Replikation auf Byte-Ebene und überprüft replizierte Daten automatisch auf als funktionierend bekannten Produktionsservern, um die Datenintegrität zu gewährleisten.

Microsoft

Online Services Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

*Durch
Kontinuität
bleiben Dienste
und Daten
verfügbar und
Ihr Geschäft
bleibt am
Laufen.*

Der Schutz der Daten verläuft fast kontinuierlich, und durch Echtzeitüberwachung können Administratoren den aktuellen Sicherungsstatus einsehen.

Neben den normalen Sicherungs- und Wiederherstellungsprozeduren wird von den Diensten der Business Productivity Online Standard Suite etwa 30 Prozent des gesamten Festplattenspeicherplatzes für Redundanz zugewiesen. Eine Kombination aus RAID5 und RAID1 sorgt für schnellen und zuverlässigen Festplattenzugriff, und die Festplattenarrays verfügen über Zusatzlaufwerke, um alle Fehlerquellen in der Konfiguration zu eliminieren.

Neben der Verhinderung von Datenverlust ist das Ziel des Diensts die Aufrechterhaltung der Datenleistung. Datenbanken werden regelmäßig auf folgende Aspekte überprüft:

- Blockierte Prozesse
- Paketverlust
- Prozesse in der Warteschlange
- Abfragelatenz

Präventive Wartung umfasst Prüfungen der Datenbankkonsistenz, periodische Datenkomprimierung sowie Überprüfungen von Fehlerprotokollen.

Verfügbarkeit und Kontinuität

Hohe Verfügbarkeit erfordert proaktive Prozeduren, um sicherzustellen, dass Probleme bei ihrer Entstehung angegangen werden, bevor sie Auswirkungen für die Kunden haben. Das Ziel ist, Schwachstellen zu erkennen und Abhilfe zu schaffen, bevor es für Kunden zu Problemen kommt.

99,9-prozentige Zuverlässigkeit

Für Microsoft Online Services wurde 99,9-prozentige Zuverlässigkeit gemessen. N+1-Redundanz bedeutet, dass wichtige Komponenten des gesamten Diensts –auf Ebene des Netzwerks, des Datenspeichers und der Anwendungsserver – dupliziert werden, um Fehler zu verhindern. Details wie duale Stromversorgungen und Netzwerkschnittstellen erhöhen die Betriebszeit für Schlüsselkomponenten noch weiter. Darüber hinaus werden Konfigurationen zwischen Datacentern extern repliziert, sodass die Datacenter selbst geschützt sind.

Vermeiden von Ressourceneinschränkungen durch Skalierbarkeit

Die Business Productivity Online Standard Suite verfügt über überschüssige Kapazitäten. Allen Benutzern werden die erforderlichen Ressourcen zugewiesen, und zusätzliche Kapazität kann proaktiv online gestellt werden, um Einschränkungen bei den momentanen Ressourcen entgegenzuwirken. Dadurch können Sie jederzeit mit sofortiger Wirkung Benutzer, Speicher oder Dienste hinzufügen.

Um unvorhersehbare Kapazitätsengpässe zu vermeiden, wird die Kapazität durch fortschrittliche Modellierungstechniken anhand von Prognosen mindestens drei Monate im Voraus optimiert. Die Kapazität wird regelmäßig auf Bedarf geprüft, um zu verhindern, dass Ressourceneinschränkungen den Dienst beeinträchtigen.

Dedizierter Support

Die Entwicklungs- und Betriebsteams von Microsoft Online Services werden durch eine dedizierte Online Services-Supportorganisation unterstützt, die eine Schlüsselrolle bei der Gewährleistung der Geschäftskontinuität für Kunden spielt. Das Supportpersonal verfügt über fundiertes Fachwissen zu den Diensten und zugehörigen Anwendungen sowie über direkten Zugang zu unternehmensweiten Microsoft-Experten für Architektur, Entwicklung und Tests.

Die Supportorganisation ist eng am Betrieb und der Produktentwicklung ausgerichtet und bietet kurze Lösungszeiten sowie einen Kanal für Mitteilungen von Kunden. Das Kundenfeedback wird bei Prozessen bezüglich Planung, Entwicklung und Betrieb berücksichtigt.

Kunden müssen sich auf die Behebung ihrer Probleme verlassen und die zeitnahe Lösung mitverfolgen können. Die Microsoft Online Services-Verwaltungskonsole bietet eine kompakte webbasierte Schnittstelle zum Support, von der aus Kunden Tickets hinzufügen und überwachen sowie Feedback von Supportpersonal erhalten können.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Minimieren von Datenverlust, Maximieren der Datenverfügbarkeit: beides gehört zusammen.

Über dieses Portal können Kunden ihre Online Services einfach verwalten, da hierbei Verwaltungsfunktionen – z. B. das Hinzufügen und Entfernen von Benutzern und Diensten – mit Supportfunktionen – das Eingeben und Überwachen von Problemtickets – miteinander kombiniert werden.

Selbsthilfe gestützt durch kontinuierlichen Personalsupport

Das Ziel für Microsoft und Kunden der Business Productivity Online Standard Suite ist Selbsthilfe, um die Notwendigkeit für Support soweit möglich zu vermeiden. Vor der Eingabe eines Tickets können Kunden auf Knowledge Base-Artikel und häufig gestellte Fragen zugreifen, die bei den meisten Problemen sofortige Hilfe bieten. Diese Ressourcen werden kontinuierlich mit den neuesten Informationen aktualisiert, wodurch Verzögerungen bei der Bereitstellung von Lösungen für bekannte Probleme vermieden werden.

Wenn jedoch ein Problem auftritt, das die Hilfe eines Supportmitarbeiters erfordert, steht Personal für unmittelbare Hilfe telefonisch oder über das Verwaltungsportal täglich rund um die Uhr zur Verfügung.

Kompatibilität

Aufgrund von Gesetzen und Bestimmungen unterliegen alle Unternehmen bedeutenden Herausforderungen bezüglich Informationssicherheit, Datenschutz, Zuverlässigkeit und geschäftlicher Integrität. Kompatibilität bedeutet im Allgemeinen die Einhaltung aller rechtlichen und geschäftlichen Anforderungen, die für eine Organisation bei der Ausführung ihrer Geschäfte gelten. Die zunehmende Zahl der Regulierungen – zusammen mit der stark gestiegenen Erzwingungsaktivität – hebt die Notwendigkeit für interne Führungsrichtlinien und -prozeduren hervor, sowohl direkt als auch durch die Dienstanbieter einer Organisation. Zahlreiche firmeneigene Richtlinien (wie z. B. Beschaffung, Qualitätssicherung und Neueinstellung) fügen eine weitere Ebene an Komplexität zu den Kompatibilitätsanforderungen hinzu, die eine Organisation zu verwalten hat.

Die Kompatibilitätsstrategie der Business Productivity Online Standard Suite basiert auf einem proaktiven kontinuierlichen Kompatibilitätsansatz zur Minderung von Risiken und zum Schutz der Umgebung. Dies wird gestützt durch regelmäßige unabhängige Prüfungen durch Dritte, um Microsoft-Kunden mehr Sicherheit zu gewährleisten.

Mit den Kompatibilitätszielen der Business Productivity Online Standard Suite wird Folgendes sichergestellt:

- Online Services stimmt mit Microsoft-Sicherheitsrichtlinien und relevanten Industriestandards überein
- Online Services erfüllt vertragliche Sicherheits- und Kompatibilitätsverpflichtungen gegenüber den Kunden

Auf Standards basierende Kompatibilitätsverwaltung

Das Kompatibilitätsteam der Business Productivity Online Standard Suite folgt dem risikobasierten Ansatz und kontinuierlichen Optimierungsprozess der International Standards Organization (ISO). Das Team bewertet die Kompatibilität von Sicherheitsimplementierungen anhand einer Methode, die auf den Richtlinien von ISO 27001 basiert.

Eine zentrale, standardisierte Grundlage für Prüfungskontrollen ist eine wesentliche Komponente eines koordinierten Kompatibilitätsverwaltungsprogramms. Das Kompatibilitätsteam der Business Productivity Online Standard Suite verwendet ein allgemeines Kontrollframework basierend auf ISO 27001. Dies ist die Grundlage für sorgfältige Business Productivity Online Standard Suite-Sicherheitskontrollen, wodurch Business Productivity Online Standard Suite-Entwickler bei Bedarf schnell neue Kontrollen implementieren können.

Kompatibilitätsverwaltungsprogramm von Microsoft Online Services

Üblicherweise gibt es einen hohen Grad an Gemeinsamkeit unter scheinbar unterschiedlichen Anforderungen bezüglich Bestimmungen und Richtlinien, die Prozesse, Kontrollen und Technologie umfassen können. Durch die effiziente Nutzung dieser Gemeinsamkeiten entsteht ein Wettbewerbsvorteil für die Kompatibilitätsfunktion innerhalb einer Organisation.

Für einen effizienteren Prozess der Verwaltung verschiedener technischer Kontrollen ermittelt Microsoft Überschneidungen bei den technischen oder prozessbasierten Kontrollen, die zu diesen Anforderungen führen, und implementiert, wenn möglich, eine einzelne Kontrolle zu deren Erfüllung. Auf diese Weise erstellt Microsoft einen integrierten Satz an speziellen Kontrollzielsetzungen und fügt diese in ein konsolidiertes Framework ein.

Der Ansatz von Microsoft Online Services für Kompatibilität besteht darin, Kompatibilitätsrisiken proaktiv zu erkennen und eine Kultur der kontinuierlichen Einhaltung innerhalb der Microsoft Online Services-Organisation zu schaffen.

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

Diese allgemeinen Kontrollen sind in die folgenden Domänen bzw. Kompetenzen gegliedert:

- Sicherheitsrichtlinien
- Organisation der Informationssicherheit
- Objektmanagement
- Personalverwaltungssicherheit
- Physische und ökologische Sicherheit
- Kommunikations- und Betriebsverwaltung
- Zugriffssteuerung
- Beschaffung, Entwicklung und Verwaltung von Informationssystemen
- Verwaltung von Informationssicherheitsvorfällen
- Verwaltung der Geschäftskontinuität
- Kompatibilität

Microsoft überprüft das allgemeine Kontrollframework regelmäßig in Bezug auf Änderungen an Industriestandards sowie an den unterschiedlichen Rechts- oder Bestimmungsumgebungen, in denen die Kunden geschäftlich tätig sind.

Das Kompatibilitätsframework von Microsoft Online Services

Von Microsoft wurde ein frameworkbasierter Ansatz für die Verwaltung von Kompatibilitätskontrollen implementiert. Durch diesen Ansatz verfügt das Microsoft-Personal über folgende Fähigkeiten:

- Effizientes Planen, Bereitstellen, Betreiben und kontinuierliches Verwalten von Kompatibilitätsanforderungen
- Erstellen technischer und prozessbasierter Kontrollen zur Erfüllung von Kundenanforderungen auf der Grundlage verschiedener regulativer Standards wie SOX und HIPAA
- Vorausplanen für neu entstehende Kundenanforderungen
- Vermeiden von doppelter Arbeit, Redundanz oder Konflikten innerhalb von Microsoft Online Services durch Bereitstellung effektiv geplanter Kompatibilitätslösungen, die in der Organisation kommuniziert werden
- Effizienteres Aktualisieren derzeitiger Kompatibilitätsanforderungen durch kontrollierte Bereitstellung schrittweiser Änderungen an den vorhandenen Kontrollen
- Einrichten und Verwalten einer gemeinsamen Grundlage für Microsoft Online Services, Kunden und Auditoren

Durch fortlaufende interne und externe Überprüfung wird das Kundenvertrauen in den Microsoft-Kompatibilitätsprozess aufrechterhalten.

Bewertungen und Überprüfungen der Kompatibilität

Das interne Microsoft-Kompatibilitätsteam ist für das Überprüfen, Überwachen, Verwalten und Abschließen von Überprüfungsproblemen verantwortlich. Dazu führt das Team regelmäßig Bewertungen von Mitarbeitern, Prozessen und Technologiekontrollen durch, um die betriebliche Effektivität zu bewerten.

Die Kompatibilitätsbewertung umfasst mehrere Phasen:

1. **Planung.** In der Planungsphase der Bewertung werden Umfang und anwendbare Kontrollen definiert.
2. **Bewertung.** Die Effektivität von Kontrollen wird gemessen und gemeldet. Die Microsoft-Prozesse zur Kompatibilitätsbewertung umfassen Mitarbeiter, Prozesse und Technologiekontrollen. Je nach Kontrolle wird die Kontrolleffektivität anhand der folgenden allgemeinen Überprüfungspraktiken bewertet:
 - **Anfrage.** Auditoren holen Informationen von sachkundigen Personen innerhalb oder außerhalb der Organisation ein.
 - **Inspektion.** Auditoren untersuchen Datensätze oder Dokumente, ob intern oder extern, in Papierform, elektronischer oder anderweitiger Form.
 - **Beobachtung.** Auditoren verfolgen einen Prozess oder eine Prozedur nach, die von den Microsoft Online Services-Betriebsteams durchgeführt wird.
3. **Korrektur.** Das Team entwickelt einen Korrekturplan anhand der Ergebnisse der Überprüfung. Die Ergebnisse werden bis zu ihrer Bearbeitung nachverfolgt. Die Serviceteams der Business Productivity Online Standard Suite sind für den Korrekturplan und dessen Umsetzung verantwortlich, und alle verbleibenden Risiken werden dem Führungsstab mitgeteilt.
4. **Berichterstellung.** Nach Abschluss aller Tests stellt Microsoft die Ergebnisse in einem Bericht zusammen. In diesem Bericht sind alle Mängel enthalten, die bei der Überprüfung festgestellt wurden. Normalerweise fallen Mängel in eine der folgenden Kategorien:
 - **Entwurfsmängel.** Bei dieser Art von Mängeln ermittelt Microsoft das vollständige oder teilweise Fehlen von Kontrollen für eine gegebene Aufgabe oder stellt fest, dass die Kontrollen für das entsprechende Ziel nicht ausreichend sind. Ein Beispiel für einen Mangel beim Entwurf ist, wenn die Organisation vertrauliche Kundeninformationen wie Name, Adresse und Führerscheinnummer verwaltet, jedoch über keinen definierten Prozess zum Schutz dieser persönlichen Informationen verfügt.
 - **Betriebsmängel.** Bei dieser Art von Mängeln stellt Microsoft fest, dass die Kontrollen nicht wie vorgesehen angewendet werden. Diese Situation kann eintreten, wenn die Kontrolle zwar dokumentiert, jedoch nie in der Produktion umgesetzt wurde, oder wenn die Kontrolle in die Produktion integriert ist, jedoch nicht befolgt wird. Beispielsweise kann eine Kontrolle besagen, dass Manager eine Benutzerzugriffsanforderung für eine bestimmte vertrauliche Ressource erst genehmigen müssen, bevor der Benutzer Zugriff erhält. Diese Kontrolle würde einen betrieblichen Mangel aufweisen, wenn der Zugriff regelmäßig ohne eine solche Genehmigung gewährt würde.

Unabhängige Zertifizierung

Zusätzlich zu der zuvor beschriebenen internen Bewertung unterliegt die Microsoft Online Services-Organisation verschiedenen unabhängigen Kompatibilitätsüberprüfungen durch Dritte, um Kunden ein größeres Maß an Garantie zu bieten. Solche unabhängigen, objektiven Überprüfungen können auch dabei helfen, Kundenverpflichtungen bezüglich Gesetzen, Bestimmungen und Kompatibilität zu erfüllen.

Demonstrieren der Kompatibilität

Es gibt eine Reihe von Möglichkeiten, die Kompatibilität mit Standards zu demonstrieren. Zwei vorwiegende Methoden sind das Statement of Auditing Standard (SAS) 70 Type II und die ISO 27001-Zertifizierung.

SAS 70 hilft Microsoft und seinen Kunden ebenfalls dabei, die Gesetzgebung des Sarbanes-Oxley Act (SOX) für die Verwaltung elektronischer Datensätze einzuhalten.

Die Microsoft-Strategie besteht darin, Online Services unabhängigen und unparteiischen Kompatibilitätsüberprüfungen und Zertifizierungen durch Dritte zu unterziehen, um den Entwurf von Kontrollen und die betriebliche Effektivität zu bestätigen, von der Dienstentwicklung bis hin zur physischen Bereitstellung von Infrastruktur und Vorgängen. Durch diese unabhängige Absicherung können Kunden nicht nur auf die Sicherheit von Diensten der Business Productivity Online Standard Suite vertrauen, sondern in einigen Fällen gleichzeitig ihre Verpflichtungen bezüglich Gesetzen, Bestimmungen und Kompatibilität erfüllen.

Darüber hinaus können Kunden dank dieser Überprüfungen durch Dritte Geld sparen, da sie keine eigenen Prüfungen durchführen müssen. Gleichzeitig wird eine bessere Überprüfung der Kontrolle von Diensten der Business Productivity Online Standard Suite durch eine unabhängige Entität sichergestellt.

Microsoft entwickelt Kompatibilitätsstrategien basierend auf der Art des Dienstangebots. In der aktuellen Reihe verfügen die Dienste jeweils über mindestens eines der folgenden Prädikate:

- Statement of Auditing Standard (SAS) 70 Type II
- ISO 27001-Zertifizierung
- Verizon Security Management Program – Service Provider Certification (zuvor Cybertrust)

Statement of Auditing Standard (SAS) 70

SAS 70 ist eine Abkürzung für Statement on Auditing Standard Number 70, entwickelt und verwaltet durch das American Institute of Certified Public Accountants (AICPA).

Genauer handelt es sich bei SAS 70 um einen „Bericht zur Verarbeitung von Transaktionen durch Dienstleistungsorganisationen“. SAS 70 ist eine umfassende Überprüfung, die gegenüber Kunden und Partnern der Dienstleistungsorganisation Transparenz demonstriert. Obwohl SAS 70-Überprüfungen und -Berichte kosten- und zeitintensiv sein können, haben sie deutliche Vorteile für die Dienstleistungsorganisationen, die sie in Anspruch nehmen.

Kompatibilität mit SAS 70 demonstriert, dass der Dienstanbieter sorgfältig von einer unabhängigen Partei geprüft wurde und über zufriedenstellende Kontrollen und Sicherheitsmaßnahmen beim Hosten oder Verarbeiten von Kundendaten verfügt. Auf diese Weise werden Transparenz sowie das Vertrauen der Kunden gefördert.

ISO 27001

ISO 27001 ist der formale Standard, mit dem Organisationen ihre Verwaltungssysteme für Informationssicherheit unabhängig zertifizieren lassen können. Darin sind Anforderungen für die Implementierung von Sicherheitskontrollen festgelegt, die an die Bedürfnisse von

Microsoft

Online Services Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services

*Ihre
Erwerbungen
bezüglich
Microsoft
Online
Services sind
durch
Kompatibilität
mit Payment
Card Industry
(PCI)
geschützt.*

einzelnen Organisationen oder Teilen davon angepasst werden. Spezielle Informationssicherheitskontrollen werden dabei nicht vorgeschrieben.

Der ISO 27001-Standard ist für die Verwaltung von Informationssicherheit etabliert und international anerkannt. Er ist im Bereich der Informationssicherheit inzwischen der am weitesten verbreitete Standard. Verschiedene Zertifizierungsinstitutionen sind von nationalen Normungsinstitutionen anerkannt (z. B. British Standards Institution und National Institute of Science and Technology), um die Kompatibilität mit ISO 27001 zu überprüfen und Zertifikate auszustellen.

Verizon Security Management Program – Service Provider Certification

Kunden, die einen Onlinedienst in Betracht ziehen, müssen darauf vertrauen können, dass die Behauptungen eines Dienstansbieters auch tatsächlich umgesetzt werden, um Kundendaten wirksam zu schützen.

Die Microsoft Online Services-Umgebung wurde durch unabhängige Überprüfungen zertifiziert, die vom Verizon Security Management Program (Service Provider Certification), zuvor Cybertrust, bereitgestellt und durchgeführt werden.

Es ist nicht möglich, die 100-prozentige Sicherheit eines Diensts zu garantieren, da sich Bedrohungen mit der Zeit weiterentwickeln. Microsoft tritt Bedrohungen jedoch mit vierteljährlichen Überprüfungen und monatlichen Tests durch interne Sicherheitsvorgänge sehr entschieden entgegen.

Aktueller und zukünftiger Status von Online Services-Zertifizierungen durch Dritte

Die Microsoft-Kompatibilitätsstrategie mit unabhängiger Überprüfung umfasst die Erlangung der ISO 27001-Zertifizierung für alle Microsoft Online Services.

Um dieses Ziel zu erreichen, startete Online Services mit der ISO 27001-Zertifizierung für die Einrichtungsverwaltung und die physische Sicherheit der eigenen Datacenter sowie verbundenen Datacenter und Infrastrukturdiensten. Die Dienste der Business Productivity Online Standard Suite selbst werden derzeit entweder der SAS 70-Bewertung unterzogen oder verfügen über die Verizon Security Management Program-Zertifizierung. Beides setzt voraus, dass eine Teilmenge von ISO-Kontrollen implementiert und in Betrieb ist.

Für die Zukunft möchte Microsoft eine End-to-End-ISO-Zertifizierung der Online Services erreichen.

Weitere Informationen

Weitere Informationen zu den in diesem Whitepaper behandelten Themen finden Sie unter den folgenden Links.

Microsoft Online Services

- [Online Services von Microsoft](http://www.microsoft.com/online) (www.microsoft.com/online)
- [Informationen zu Microsoft Online Services](http://www.microsoft.com/resources/technet/en-us/MSONline/Microsoft%20Online%20Services/html/99d9ede5-ce15-476c-9a3f-d42a481d287e.htm) (www.microsoft.com/resources/technet/en-us/MSONline/Microsoft Online Services/html/99d9ede5-ce15-476c-9a3f-d42a481d287e.htm)
- [Microsoft-Lösungen für Hostinganbieter](http://www.microsoft.com/serviceproviders/hostingproviders.mspix) (www.microsoft.com/serviceproviders/hostingproviders.mspix)
- [Microsoft Datacenters](http://blogs.technet.com/msdatacenters/)-Blog (blogs.technet.com/msdatacenters/)

Sicherheit und Dienstkontinuität

- [Microsoft Security Central](http://www.microsoft.com/security/default.mspix) (www.microsoft.com/security/default.mspix)
- [Microsoft Operations Framework](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/default.mspix) (www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/default.mspix)
- [Windows Server 2003 Security Services](http://www.microsoft.com/windowsserver2003/technologies/security/default.mspix) (www.microsoft.com/windowsserver2003/technologies/security/default.mspix)
- [Microsoft Forefront™](http://www.microsoft.com/forefront/default.mspix) (www.microsoft.com/forefront/default.mspix)
- [Bewährte Methoden für die Dienstkontinuität](http://technet.microsoft.com/de-de/library/bb633282.aspx) (technet.microsoft.com/de-de/library/bb633282.aspx)

Datenschutz

- [The Microsoft Trustworthy Computing Privacy Overview](http://www.microsoft.com/mscorp/twc/privacy/default.mspix) (www.microsoft.com/mscorp/twc/privacy/default.mspix)
- [Entwicklungszyklus für sichere Software](http://msdn2.microsoft.com/de-de/library/ms995349.aspx) (msdn2.microsoft.com/de-de/library/ms995349.aspx)
- [Microsoft Online Services Privacy Statement](http://go.microsoft.com/fwlink/?LinkId=143471) (go.microsoft.com/fwlink/?LinkId=143471)
- [Privacy Guidelines for Developing Software Products and Services](http://go.microsoft.com/fwlink/?LinkId=143469) (go.microsoft.com/fwlink/?LinkId=143469)

Kompatibilität

- [Security Compliance Management Toolkit](http://www.microsoft.com/downloads/details.aspx?FamilyId=5534BEE1-3CAD-4BF0-B92B-A8E545573A3E&displaylang=en) (www.microsoft.com/downloads/details.aspx?FamilyId=5534BEE1-3CAD-4BF0-B92B-A8E545573A3E&displaylang=en)

Microsoft

Online Services

Sicherheit in der Business Productivity Online Standard Suite von Microsoft Online Services