

Sicherheit in der Cloud von Microsoft Infrastruktur

In diesem Whitepaper stellen wir das Online Services Security- und Compliance-Team vor, das die Sicherheitstechnologie für die Microsoft Cloud-Infrastruktur managet. Dieses Team ist Teil der Global Foundation Services. Die Leser erhalten einen Überblick darüber, was Cloud Computing bei Microsoft heute bedeutet, und wie das Unternehmen eine zuverlässige Cloud Computing-Infrastruktur bereitstellt.

Veröffentlicht: Mai 2009

Inhaltsverzeichnis

| | |
|---|----|
| Zusammenfassung..... | 3 |
| Herausforderungen beim Thema Sicherheit & Cloud Computing | 4 |
| So handhabt Microsoft diese Herausforderungen..... | 5 |
| Was ist die Microsoft Cloud Computing-Umgebung?..... | 6 |
| Online Services Security und Compliance-Team..... | 6 |
| Trustworthy Computing bei Microsoft..... | 7 |
| Datenschutz..... | 8 |
| Sicherheit..... | 9 |
| Informationssicherheitsprogramm | 9 |
| Risiko-Management-Prozesse | 11 |
| Business Continuity Management | 11 |
| Security Incident Management | 13 |
| Global Criminal Compliance | 13 |
| Betriebliche Compliance | 14 |
| Mehrstufige Abwehrstrategie | 16 |
| Physische Sicherheit | 16 |
| Netzwerksicherheit | 17 |
| Datensicherheit | 18 |
| Identitäts- und Zugriffsverwaltung..... | 18 |
| Anwendungssicherheit..... | 18 |
| Überwachung der Hostsicherheit und Berichterstellung..... | 20 |
| Fazit | 22 |
| Weitere Ressourcen | 23 |

Zusammenfassung

Jüngste Untersuchungsergebnisse zu den Begriffen „Cloud“, „Cloud Computing“ und „Cloud-Umgebung“ haben ergeben, was Kunden von Cloud- Anbietern tatsächlich erwarten. Außerdem wurden Methoden entwickelt, mit denen sich die Angebote der Anbieter kategorisieren lassen. Die Idee, dass der Kauf von Diensten aus einer Cloud-Umgebung den technischen und geschäftlichen Entscheidungsträgern unter Umständen Einsparungen und Unternehmen die Konzentration auf ihre Kerngeschäfte ermöglicht, stellt im aktuellen wirtschaftlichen Klima einen großen Anreiz dar. Viele Analysten haben trotz der neuartigen Möglichkeiten zur Preisgestaltung und Online-Bereitstellung von Diensten Bedenken bezüglich der Marktbedingungen. Diese Marktstudien und der sich daraus entwickelnde Dialog zwischen möglichen Kunden und Dienst Anbietern zeigen, dass bestimmte Themen sich als potenzielle Hindernisse zur schnellen Einführung von Cloud Services entwickelt haben. Bedenken bezüglich Sicherheit, Datenschutz und der Kontrolle über Betriebsabläufe stehen auf der Liste der potenziellen Hindernisse ganz oben. Microsoft hat verstanden, dass geschäftliche Entscheidungsträger viele Fragen zu diesen Punkten haben und wissen müssen, wie mit diesen Themen in der Cloud Computing-Umgebung bei Microsoft umgegangen wird. Darüber hinaus müssen Kunden wissen, wie sich das auf ihr eigenes Risiko und ihre geschäftlichen Entscheidungen auswirkt.

In diesem Dokument erfahren Sie, wie der koordinierte und strategische Einsatz von Menschen, Prozessen, Technologien und Erfahrungen zu einer stetigen Verbesserung der Sicherheit der Cloud-Umgebung von Microsoft führt. Das OSSC-Team (Online Services Security and Compliance) baut innerhalb des Global Foundation Services auf denselben Sicherheitsprinzipien und Prozessen auf, die Microsoft in jahrelanger Erfahrung im Management von Sicherheitsrisiken in der herkömmlichen Entwicklung und bei Betriebsumgebungen gesammelt hat.

Herausforderungen beim Thema Sicherheit & Cloud Computing

Die Informationstechnologiebranche sieht sich auch mit Herausforderungen konfrontiert, die mit den Möglichkeiten von Cloud Computing einhergehen. Seit über 15 Jahren beschäftigt sich Microsoft mit den folgenden Herausforderungen bei der Bereitstellung von Online Services:

- **Neuartige Cloud-Geschäftsmodelle erzeugen eine zunehmende gegenseitige Abhängigkeit zwischen dem öffentlichen und privaten Sektor und den dort arbeitenden Menschen:** Solche Organisationen/Unternehmen und ihre Kunden werden durch die Nutzung von Clouddiensten immer abhängiger voneinander. Mit diesen neuen Abhängigkeiten gehen gegenseitige Erwartungen einher, dass Plattform-Services und gehostete Anwendungen sicher und verfügbar sind. Microsoft bietet eine zuverlässige Infrastruktur, eine Grundlage, auf der Einheiten des öffentlichen und des privaten Sektors und ihre Partner eine vertrauenswürdige Basis aufbauen können. Microsoft arbeitet aktiv mit diesen Gruppen und den Entwicklern zusammen, um die Einführung sicherheitsorientierter Risikomanagementprozesse voranzutreiben.
- **Die stetig fortschreitende Einführung von Cloud Services, einschließlich der fortschreitenden Entwicklung von Technologien und Geschäftsmodellen, erzeugt eine dynamische Umgebung, die in sich schon eine Herausforderung an die Sicherheit ist:** Schritt halten mit dem Wachstum und zukünftige Bedürfnisse vorhersehen, das sind zentrale Aspekte beim Ausführen eines effektiven Sicherheitsprogramms. Veränderungen haben bereits mit der steigenden Bedeutung von Virtualisierung und einer zunehmenden Adaption der Software plus Services-Strategie von Microsoft begonnen, die Leistungsfähigkeit und Funktionen von Computern, mobilen Geräten, Online Services und Unternehmenssoftware miteinander verbindet. Die Einführung der Cloud-Plattformen ermöglicht die Entwicklung kundenspezifischer Anwendungen, auch durch Dritte, und eine Bereitstellung in der Microsoft Cloud. Über das Informationssicherheitsprogramm für Online Services, das später in diesem Dokument detailliert beschrieben wird, pflegt Microsoft starke Partnerschaften zwischen Sicherheits-, Produkt- und Serviceteams und bietet eine zuverlässige Microsoft Cloud-Umgebung vor dem Hintergrund dieser Veränderungen.
- **Versuche, Online Service-Angebote zu unterbrechen oder in diese einzubrechen, werden immer ausgeklügelter, da in diesem illegalen Bereich immer mehr Profit gesehen wird.** Während es immer noch einfache Attacken wie unrechtmäßige Domainenreservierung oder Man-in-the-Middle-Angriffen gibt, nehmen ausgeklügeltere bösartige Attacken, die auf den Erwerb von Identitäten oder das Blockieren des Zugriffs auf sensible Geschäftsdaten abzielen, stetig zu, einhergehend mit einem Anstieg von organisierteren Untergrundmärkten für gestohlene Informationen. Microsoft arbeitet eng mit den Vollzugsbehörden, Branchenpartnern und Marktbegleitern, sowie Forschungsgruppen zusammen, um diese neuartigen Bedrohungen zu verstehen und zu bekämpfen. Außerdem führt der später in diesem Dokument beschriebene Microsoft Security Development Lifecycle (Entwicklungszyklus für sichere Software) Sicherheit und Datenschutz schon von Beginn an in den gesamten Entwicklungsprozess ein.
- **Komplexe Anforderungen an Compliance müssen bewältigt, und neue, vorhandene Dienste weltweit bereitgestellt werden:** Die Einhaltung behördlicher und gesetzlicher (im restlichen Teil dieses Papers einfach als „gesetzlich“ bezeichnet) und branchenspezifischer Vorschriften ist ein sehr komplexer Bereich, da weltweit jedes Land eigene Gesetze zur Regelung der Bereitstellung und Nutzung von Online-Umgebungen erlässt. Microsoft muss eine Unmenge gesetzlicher Vorschriften einhalten, da es über Rechenzentren in vielen Ländern verfügt und einem weltweiten Kundenstamm Online Services anbietet. Zusätzlich müssen Branchenvorschriften eingehalten werden. Microsoft hat ein Compliance Framework implementiert, das weiter unten in diesem Dokument beschrieben wird, mit dem die verschiedenen Anforderungen an die Einhaltung von Vorschriften effizient verwaltet werden können, ohne eine übermäßige Belastung für Unternehmen zu schaffen.

So handhabt Microsoft diese Herausforderungen

Seit der Markteinführung von MSN[®] im Jahr 1994 hat Microsoft Online Services entwickelt und betrieben. Die GFS-Abteilung verwaltet die Cloud-Infrastruktur und -Plattform für Microsoft Online Services und stellt dabei auch die tägliche Verfügbarkeit für Hunderte von Millionen von Kunden in der ganzen Welt rund um die Uhr sicher. Mehr als 200 der Online Services und Webportale des Unternehmens werden in dieser Cloud-Infrastruktur gehostet, z. B. die bekannten kundenorientierten Dienste Windows Live™ Hotmail[®] und Live Search und die unternehmensorientierten Dienste Microsoft Dynamics[®] CRM Online und Microsoft Business Productivity Online Standard Suite der Microsoft Online Services.

Ob die persönlichen Daten eines Kunden auf seinem eigenen Computer oder in einer Online-Umgebung gespeichert werden, oder ob die unternehmenswichtigen Daten eines Unternehmens intern oder auf einem gehosteten Server gespeichert und über das Internet gesendet werden, Microsoft weiß, dass alle diese Dienste in einer vertrauenswürdigen Umgebung betrieben werden müssen. Als Unternehmen befindet sich Microsoft in der einmaligen Situation, sowohl Leitfäden als auch technische Lösungen anzubieten, die ein sichereres Onlineerlebnis gewährleisten können. Microsoft will Kunden helfen, finanzielle Verluste und andere Folgen opportunistischer und gezielter Online-Angriffe zu vermeiden. Als Bestandteil eines stetigen Engagements für Trustworthy Computing stellt Microsoft sicher, dass die im Unternehmen beschäftigten Menschen und angewendeten Prozesse und Technologien sicherere und den Datenschutz verbessernde Maßnahmen, Produkte und Dienste bieten.

Microsoft bietet eine zuverlässige Cloud durch Konzentration auf drei Bereiche:

- Nutzung eines risikobasierten Informationssicherheitsprogramms, mit dem sich Sicherheits- und betriebliche Bedrohungen für das Unternehmen auswerten und priorisieren lassen
- Wartung und Aktualisierung eines detaillierten Satzes von Sicherheitskontrollen, die Risiken mindern
- Betrieb eines Compliance Frameworks, das sicherstellt, dass Maßnahmen und Kontrollen ordnungsgemäß entwickelt werden und effektiv funktionieren

In diesem Dokument wird beschrieben, wie Microsoft Kundendaten und betriebliche Abläufe durch ein umfassendes Informationssicherheitsprogramm und eine ausgereifte Methodik für das Richtlinien- und Compliance Management, regelmäßige interne und externe Überprüfungen der Methoden und Funktionen sowie robuste Sicherheitskontrollen in allen Dienstschichten schützt. Durch diese Prozesse und Mechanismen hält Microsoft die industriespezifischen und gesetzlichen Vorgaben für alle Regularien, Richtlinien, gesetzlichen und behördlichen Vorschriften ein und bietet diese einem weltweiten Kundenstamm online an.

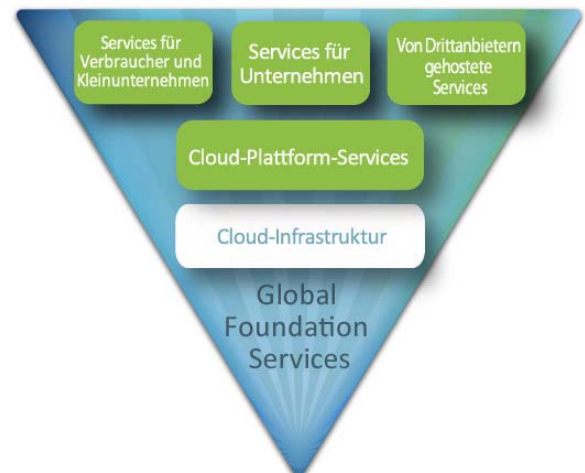
In diesem Dokument werden zwar Datenschutzrichtlinien erwähnt, es soll aber keine ausführliche Erörterung der Datenschutzrichtlinien erfolgen oder ein Leitfaden für Datenschutzvorgehensweisen gegeben werden. Informationen zu der Handhabung der Datenschutzanforderungen durch Microsoft finden Sie auf der Seite zum [Microsoft Trustworthy Computing-Datenschutz](#).

Was ist die Microsoft Cloud Computing-Umgebung?

Die Microsoft Cloud Computing-Umgebung setzt sich aus der physischen und logischen Infrastruktur sowie den gehosteten Anwendungen und Plattform-Services zusammen. GFS bietet die physische und logische Cloud-Infrastruktur bei Microsoft einschließlich vieler Plattform-Services. Die physische Infrastruktur umfasst die Rechenzentren selbst sowie die Hardware und Komponenten, die die Services und Netzwerke unterstützen. Bei Microsoft besteht die logische Infrastruktur aus Betriebssysteminstanzen, gerouteten Netzwerken und unstrukturiertem Datenspeicher, auf virtuellen wie auf physischen Objekten ausgeführt. Die Plattform-Services umfassen Rechenlaufzeiten (z. B. Internet Information Services, das .NET Framework, Microsoft[®] SQL Server[®]), Identitäts- und Verzeichnisspeicher (z. B. Active Directory[®] und Windows Live ID), Namensdienste (DNS) und andere erweiterte Funktionen, die von Online Services genutzt werden. Microsoft Cloud-Plattform-Services, z. B. Infrastrukturdienste, können virtualisiert oder physikalisch tatsächlich vorhanden sein.

Online-Anwendungen, die in der Microsoft Cloud ausgeführt werden, umfassen einfache und komplexe Produkte, die für eine Vielzahl von Kunden entwickelt wurden. Diese Online Services und die damit einhergehenden Sicherheits- und Datenschutzanforderungen können grob als Angebote für Folgendes gruppiert werden:

- **Services für Verbraucher und Kleinunternehmen:** Beispiele hierfür sind Windows Live Messenger, Windows Live Hotmail, Live Search, Xbox LIVE[®] und Microsoft Office Live.
- **Services für mittelständische und große Unternehmen:** Beispiele hierfür sind Microsoft Dynamics CRM Online und die Microsoft Business Productivity Online Standard Suite einschließlich Exchange Online, SharePoint[®] Online und Office Live Meeting.
- **Von Dritten gehostete Services:** Webbasierte Anwendungen und Lösungen, die von Dritten mit Plattform-Services entwickelt und betrieben werden, die über die Microsoft Cloud Computing-Umgebung bereitgestellt werden.



Online Services Security und Compliance-Team

Das OSSC-Team innerhalb GFS ist verantwortlich für das Informationssicherheitsprogramm der Microsoft Cloud-Infrastruktur einschließlich Richtlinien und Programmen, die zum Management der Online-Sicherheitsrisiken verwendet werden. Die Mission des OSSC-Teams ist die Ermöglichung von zuverlässigen Online Services, die Microsoft und seinen Kunden einen Wettbewerbsvorteil verschaffen. Die Positionierung dieser Funktion auf der Cloud-Infrastrukturebene ermöglicht allen Microsoft Cloud Services die Vorteile von Einsparungen und geminderter Komplexität durch die Nutzung freigegebener Sicherheitslösungen. Mit diesem standardmäßigen Ansatz können sich zudem alle Microsoft Service-Teams auf die individuellen Sicherheitsbedürfnisse ihrer Kunden konzentrieren.

Das OSSC-Team forciert die Bereitstellung einer vertrauensvollen Erfahrung in der Microsoft Cloud durch das

Informationssicherheitsprogramm von Microsoft mit einem risikobasierten Betriebsmodell und einer tiefgreifenden Abwehrstrategie für Steuerelemente. Dies umfasst regelmäßige Risikomanagementprüfungen, Entwicklung und Wartung eines Sicherheitskontroll-Frameworks sowie fortlaufende Bemühungen Compliance bei Aktivitäten von der Rechenzentren-Entwicklung bis hin zur Reaktion auf Anfragen von Vollzugsbehörden in der ganzen Welt sicherzustellen. Das Team wendet im gesamten Lebenszyklus der Online Services und in jedem Element der Infrastruktur Best Practice-Prozesse an, inklusive einer Vielzahl interner und externer Prüfungen. Die enge Zusammenarbeit mit anderen Microsoft-Teams führt zu einem umfassenden Ansatz zur Sicherung von Anwendungen in der Microsoft Cloud.

Das Betreiben einer globalen Cloud-Infrastruktur in vielen Unternehmen ist an die Notwendigkeit gekoppelt, Compliance-Verpflichtungen nachzukommen und die Überprüfung durch externe Prüfer zu bestehen. Prüfbare Anforderungen stammen aus Vorschriften von Regierungen und der Branche, internen Richtlinien und Best Practices der Branche. Das OSSC-Programm gewährleistet die ständige Bewertung und Umsetzung von Erwartungen an die Compliance. Infolge des Information Security Program kann Microsoft wichtige Zertifizierungen, wie Bescheinigungen der International Organization for Standardization/International Society of Electrochemistry 27001:2005 (ISO/IEC 27001:2005) und des Statement of Auditing Standard (SAS) 70 Typ I und Typ II, erwerben und die regelmäßigen Prüfungen durch unabhängige Dritte effizienter bestehen.

Trustworthy Computing bei Microsoft

Die wichtigste Antriebskraft beim Erstellen eines effektiven Sicherheitsprogramms ist ein ständiges Bewusstsein und eine hohe Bewertung von Sicherheit. Microsoft hat erkannt, dass eine solche Kultur von den Führungsetagen der Unternehmen beauftragt und unterstützt werden muss. Das Microsoft-Management engagiert sich schon lange für die angemessenen Investitionen und Anreize zur Förderung eines sicheren Verhaltens. 2002 rief das Unternehmen die Trustworthy Computing-Initiative ins Leben, bei der Bill Gates Microsoft verpflichtete, seine Mission und Strategie in den wichtigsten Bereichen fundamental zu verändern. Heute ist Trustworthy Computing einer der wichtigsten Unternehmenswerte bei Microsoft und eine Richtlinie für beinahe alle Aktionen des Unternehmens. Die Grundlage dieser Initiative bilden diese vier Werte: Datenschutz, Sicherheit, Zuverlässigkeit und Geschäftspraktiken. Weitere Informationen zu Trustworthy Computing finden Sie auf der Seite zu [Microsoft Trustworthy Computing](#).

Microsoft versteht, dass der Erfolg in der schnell wachsenden Branche der Online Services von der Sicherheit und dem Datenschutz der Kundendaten sowie der Ausfallsicherung der von Microsoft gebotenen Services abhängt. Microsoft entwickelt und testet Anwendungen und Infrastruktur sorgfältig anhand international anerkannter Standards, um diese Funktionen und die Einhaltung gesetzlicher Vorschriften und der internen Sicherheits- und Datenschutzrichtlinien zu demonstrieren. Kunden profitieren damit von dem optimierten Ansatz von Microsoft zu testen, zu überwachen, automatisiert Patches bereitzustellen und fortlaufend Sicherheitsverbesserungen zu realisieren.

Datenschutz

Microsoft verpflichtet sich darauf, den Datenschutz und die Sicherheit der Informationen der Kunden zu schützen und dabei alle maßgeblichen Datenschutzgesetze einzuhalten und die strikten Datenschutzpraktiken der Datenschutzbestimmungen von Microsoft zu befolgen.

Um eine vertrauenswürdige Umgebung für Kunden zu schaffen, entwickelt Microsoft Software, Services und Prozesse immer mit Blick auf den Datenschutz. Microsoft-Teams sind bei der Einhaltung der globalen Datenschutzgesetze besonders achtsam, und die Datenschutzpraktiken des Unternehmens wurden aus den Datenschutzgesetzen aus der ganzen Welt entwickelt. Microsoft hält diese Datenschutzgesetze ein und wendet diese Standards weltweit an.

Microsoft setzt sich für den Schutz der Sicherheit Ihrer Daten ein. Die Online Service-Bereitstellungsteams nutzen eine Vielzahl von Sicherheitstechniken und Vorgehensweisen, um die persönlichen Daten besser vor unerlaubtem Zugriff sowie unerlaubter Nutzung und Veröffentlichung zu schützen. Microsoft-Softwareentwicklungsteams wenden in allen Entwicklungs- und Betriebspraktiken des Unternehmens die PD3+C-Prinzipien an, die im Security Development Lifecycle (SDL) festgelegt sind:

- **Privacy by Design:** Microsoft wendet dieses Prinzip während der Entwicklung, Veröffentlichung und Wartung von Anwendungen an, um sicherzustellen, dass die von Kunden gesammelten Daten einem bestimmten Zweck dienen und die Kunden angemessen benachrichtigt werden, damit sie informierte Entscheidungen treffen können. Wenn zu sammelnde Daten als besonders vertraulich eingestuft werden, werden z. B. Maßnahmen wie Verschlüsselung bei der Übertragung und während der Speicherung ergriffen.
- **Privacy by Default:** In Angeboten von Microsoft werden Kunden um ihre Erlaubnis gebeten, bevor vertrauliche Daten gesammelt oder übertragen werden. Nach der Autorisierung werden diese Daten durch Maßnahmen wie Zugriffsteuerungslisten (ACLs) in Kombination mit Mechanismen der Identitätsauthentifizierung geschützt.
- **Datenschutz bei der Bereitstellung:** Microsoft veröffentlicht Datenschutzmechanismen im angemessenen Maß für Unternehmenskunden, damit diese angemessene Datenschutz- und Sicherheitsrichtlinien für ihre Benutzer erstellen können.
- **Kommunikation:** Microsoft arbeitet bewusst transparent und unterstützt aktiv durch die Veröffentlichung von Datenschutzrichtlinien, Whitepapers und anderen Dokumentationen, die sich auf den Datenschutz beziehen.

Weitere Informationen zum Engagement von Microsoft für den Datenschutz finden Sie auf der Seite zum [Datenschutz von Microsoft beim Trustworthy Computing](#).

Sicherheit

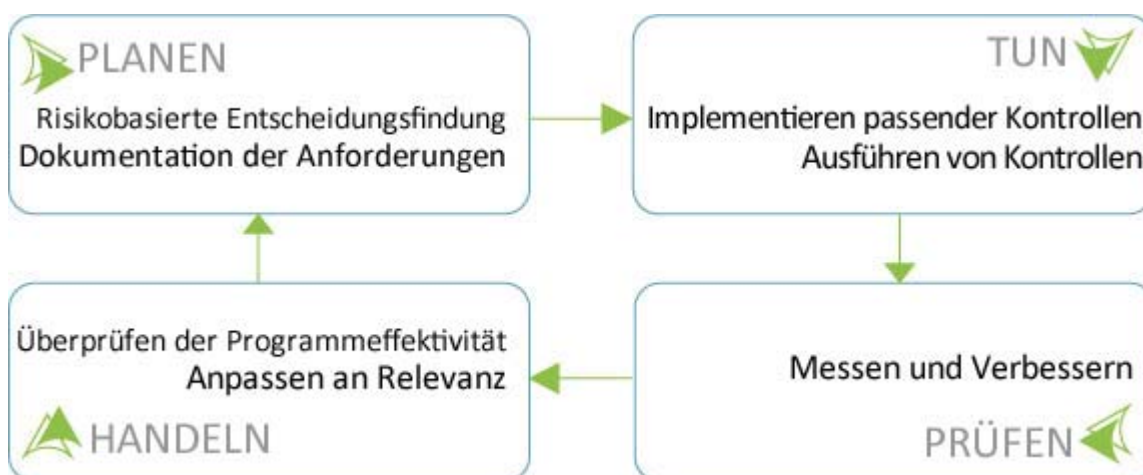
Microsoft hat seine Cloud-Infrastruktur weiter angepasst, um den Vorteil neuartiger Technologien wie Virtualisierung zu nutzen. Diese Fortschritte führen zu einer Entkoppelung der Datenressourcen von einer allgemeinen physischen Infrastruktur für viele Arten von Kundenobjekten. Der Punkt, dass der zukünftig online gehostete Softwareentwicklungsprozess für Anwendungen oft agiler ist und ständig neue Versionen bietet, führt dazu, dass das Informations-Sicherheitsrisikomanagement angepasst werden muss, damit eine Trustworthy Computing-Erfahrung geboten werden kann.

Die folgenden Abschnitte dieses Dokuments bieten Ihnen eine Einsicht in die Art und Weise, wie das Microsoft OSSC-Team Sicherheitsgrundlagen anwendet und welche Bemühungen im gesamten Unternehmen zum Management von Risiken in der Microsoft Cloud-Infrastruktur unternommen werden. Außerdem erfahren Sie hier, was eine mehrstufige Abwehrstrategie für die Online Service-Sicherheit bedeutet und wie die Cloud Computing-Umgebung zu neuen Ansätzen für Sicherheitsmaßnahmen führt.

Informationssicherheitsprogramm

Das Online-Informationssicherheitsprogramm von Microsoft legt fest, wie das OSSC-Team arbeitet. Das Programm wurde unabhängig vom British Standards Institute (BSI), Management Systems America als kompatibel mit ISO/IEC 27001:2005 zertifiziert. Die Zertifikate können im Internet auf der Seite des BSI eingesehen werden. [Certificate/Client Directory Search Results](#).

Das Informationssicherheitsprogramm organisiert die Sicherheitsanforderungen in drei Top-Level-Domänen: administrativ, technisch und physisch. Die Kriterien dieser Domänen stehen für die Grundlage, auf der das Risikomanagement erfolgt. Ausgehend von den Schutzmaßnahmen und Kontrollen, die in den Domänen und ihren Unterkategorien identifiziert werden, folgt das Informationssicherheitsprogramm dem ISO/IEC27001:2005-Framework aus „Planen, Handeln, Prüfen, Agieren“.



OSSC definiert darüber hinaus die vier Schritte in der traditionellen „Planen, Handeln, Prüfen, Agieren“-Struktur eines ISO-Informationssicherheitsprogramms wie folgt:

- **Planen**
 - a. **Risikobasierte Entscheidungsfindung:** Durch Antreiben der Priorisierung wichtiger Aktivitäten und Zuweisung von Ressourcen erstellt OSSC einen Sicherheitsmaßnahmenplan auf der Grundlage von Risikobewertungen. Die in diesem Plan erfassten Ziele des Unternehmens und von Einzelnen umfassen Aktualisierungen von Richtlinien, Betriebsstandards und Sicherheitskontrollen in GFS und vielen Produktgruppen.
 - b. **Dokumentanforderungen:** OSSC setzt klare Erwartungen, die die Voraussetzungen für den Erwerb von Bescheinigungen und Zertifizierungen Dritter durch ein dokumentiertes Kontroll-Framework schaffen. Dieses Framework bietet Anforderungen auf eine eindeutige, einheitliche und präzise Weise.
- **Handeln**
 - a. **Einführen angemessener Kontrollen:** Kontrollen auf der Grundlage des Sicherheitsmaßnahmenplans werden von Betriebs-, Produkt- und Dienstbereitstellungsteams eingeführt.
 - b. **Betriebliche Kontrollen:** OSSC implementiert und betreibt viele Kontrollen direkt, z. B. Kontrollen zur Gewährleistung von Global Criminal Compliance, zum Management der Bedrohung für die Infrastruktur und zur physischen Sicherung von Rechenzentren. Weitere Maßnahmen werden von Betriebs-, Produkt- und Dienstbereitstellungsteams eingeführt und aufrechterhalten.
- **Prüfen**
 - a. **Messen und Verbessern:** OSSC bewertet die Kontrollaktivität ständig. Zusätzliche Kontrollen können hinzugefügt oder vorhandene geändert werden, damit die Erfüllung der in der Informationssicherheitsrichtlinie aufgeführten Ziele und des Kontroll-Frameworks sichergestellt sind.
- **Agieren**
 - a. **Überprüfen der Effektivität des Programms:** Sowohl interne Teams als auch externe Prüfer überprüfen regelmäßig das Informationssicherheitsprogramm als Bestandteil der fortlaufenden Bemühungen, die Effektivität des Programms sicherzustellen.
 - b. **Anpassen, um relevant zu bleiben:** OSSC bewertet das Informationssicherheitsprogramm und sein Kontroll-Framework mithilfe der anwendbaren gesetzlichen, geschäftlichen und branchenspezifischen Anforderungen und Standards, um verbesserungswürdige Bereiche zu erkennen und zu überprüfen, ob Ziele erreicht werden. Daher werden die Technologie und Geschäftspläne von Microsoft zur Inangriffnahme der Auswirkungen betrieblicher Änderungen aktualisiert.

Sicherheitsprogramme sind erst dann vollständig, wenn sie auch die Notwendigkeit der Mitarbeiterschulung umfassen. Microsoft erstellt und bietet Sicherheitstrainings an und stellt somit sicher, dass alle Gruppen, die an der Erstellung, Bereitstellung, Betreuung und Unterstützung von in der Cloud-Infrastruktur gehosteten Online Services beteiligt sind, ihre Verantwortung im Zusammenhang mit der Informationssicherheitsrichtlinie für Online Services bei Microsoft verstehen.

Dieses Schulungsprogramm lehrt die wichtigsten Leitprinzipien, die angewendet werden sollten, wenn die einzelnen Ebenen der mehrstufigen Abwehrstrategie von Microsoft zum Sichern von Online Services betrachtet werden. Microsoft fordert zudem Geschäftskunden und externe Softwareentwickler dazu auf diese Prinzipien anzuwenden, wenn sie Anwendungen entwickeln und Dienste mit der Microsoft Cloud-Infrastruktur bereitstellen.

Risiko-Management-Prozesse

Die Analyse und Behebung von Sicherheitsrisiken in voneinander abhängigen Online-Systemen ist komplexer und kann zeitaufwändiger sein als die in herkömmlichen IT-Systemen. Risikomanagement und die damit einhergehenden Überprüfungen müssen an diese dynamische Umgebung angepasst werden. Microsoft nutzt ausgereifte Prozesse auf der Grundlage langjähriger Erfahrung im Bereitstellen von Diensten im Internet, um diese neuen Risiken zu bewältigen.

Die OSSC-Mitarbeiter arbeiten zusammen mit Betriebsteams, Geschäftsbereichen und Dienstbereitstellungsgruppen bei Microsoft am Management dieser Risiken. Das Informationssicherheitsprogramm etabliert die Standardprozesse und Dokumentationsanforderungen zur Durchführung fortlaufender risikobasierter Entscheidungsfindung.

Durch das Sicherheitsrisikomanagement-Programm (SRMP) erfolgen Risikobewertungen auf einer Vielzahl von Ebenen und werden Priorisierungen in Bereichen wie Produktveröffentlichungsplänen, Richtlinien Einhaltung und Ressourcenzuweisung vorgenommen. Jährlich erfolgt eine umfassende Bewertung der Risiken für die Microsoft Cloud-Infrastruktur mit anschließenden unterjährigen, kontinuierlichen Überprüfungen. Diese fortlaufende Arbeit konzentriert sich auf besondere Risiken. Durch diesen Prozess priorisiert und leitet Microsoft die Entwicklung von Sicherheitskontrollen und begleitenden Aktivitäten. Die SRMP-Methodik bewertet die Effektivität der Kontrollen gegenüber Risiken durch:

- Identifizierung von Bedrohungen und Risiken für die Umgebung
- Risikoberechnung
- Berichterstattung über Risiken in der gesamten Microsoft Cloud-Umgebung
- Maßnahmen gegen Risiken auf der Grundlage der Auswirkungsbewertung und des damit zusammenhängenden Unternehmensfalls
- Testen der Effektivität der Maßnahmen und des Restrisikos
- Fortlaufendes Risikomanagement

Business Continuity Management

Viele Unternehmen, die eine Nutzung von Cloud-Anwendungen in Betracht ziehen, haben Fragen zu der Verfügbarkeit und Ausfallsicherheit der Dienste. Das Hosten von Anwendungen und Speichern von Daten in einer Cloud-Umgebung bietet neue Möglichkeiten der Verfügbarkeit und Ausfallsicherheit von Diensten sowie der Datensicherung und -wiederherstellung. Das Programm zum Business Continuity Management von Microsoft nutzt die Best Practices der Branche zum Erstellen und Anpassen von Funktionen in diesem Bereich für neue Anwendungen, die in der Microsoft Cloud-Umgebung zur Verfügung gestellt werden.

Microsoft wendet einen fortlaufenden Management- und Governance-Prozess an, mit dem es sicherstellt, dass die zur Identifizierung der Wirkung möglicher Verluste, zur Einhaltung geeigneter Wiederherstellungspläne und -strategien und zur Gewährleistung der Kontinuität der Produkte und Dienste erforderlichen Schritte unternommen werden. Es ist wichtig, alle Ressourcen – Menschen, Geräte und Systeme – zu kennen, die zur Ausführung einer Aufgabe oder Durchführung eines Prozesses erforderlich sind, damit ein entsprechender Plan für Notfälle erstellt werden kann. Diesen Plan nicht zu prüfen, zu warten und zu testen ist eines der größten Risiken, das zu Verlusten von verheerenden Ausmaßen führen kann, und daher endet das Programm nicht mit der einfachen Aufzeichnung von Wiederherstellungsmaßnahmen. Microsoft erstellt und wartet mithilfe des Entwicklungszyklus des Business Continuity Management Wiederherstellungspläne durch die Anwendung von sechs Phasen, wie in der folgenden Abbildung dargestellt:



Microsoft nimmt sich der Wiederherstellung von Diensten und Daten an, nachdem eine Abhängigkeitsanalyse durch Identifizierung von zwei Zielen in Bezug auf die Wiederherstellung der Ressourcen durchgeführt wurde:

- **Recovery Time Objective (RTO):** Die maximale Dauer, die der Verlust von wichtigen Prozessen, Funktionen oder Ressourcen anhalten kann, bevor daraus ein schwerwiegender geschäftlicher Nachteil entstünde.
- **Recovery Point Objective (RPO):** Die maximale Datenmenge, deren Verlust in einem Notfall ausgeglichen werden kann. In der Regel wird dies als die Zeit zwischen der letzten Datensicherung und dem Ausfall definiert.

Da der Prozess der Identifizierung und Klassifizierung von Ressourcen als Bestandteil des Risikomanagements für die Microsoft Cloud Computing-Infrastruktur fortlaufend ist, bedeutet der Plan zur Notfallwiederherstellung, dass diese Ziele einfacher zur Bewertung angewendet werden können, ob oder ob nicht in einem Notfall Wiederherstellungsmaßnahmen zu ergreifen sind. Microsoft überprüft diese Strategien außerdem durch Ausführung von Übungen, die Proben, Tests, Schulungen und Wartung umfassen.

Security Incident Management

Die Sicherheitskontrollen und Risikomanagementprozesse, die Microsoft zur Sicherung der Cloud-Infrastruktur unterhält, mindern die Risiken von Sicherheitsvorfällen. Es wäre jedoch unrealistisch zu denken, dass zukünftig keine bösartigen Angriffe erfolgen werden. Das Security Incident Management, kurz SIM-Team, im OSSC reagiert auf diese Probleme, wenn sie auftreten. Dieses Team arbeitet täglich rund um die Uhr. Die Mission von SIM ist die schnelle und akkurate Bewertung und Behebung von Computersicherheitsvorfällen im Zusammenhang mit Microsoft Online Services bei gleichzeitiger klarer Kommunikation der relevanten Informationen an die Geschäftsführung und andere betroffene Stellen bei Microsoft.

Es gibt sechs Phasen im SIM-Vorfallsreaktionsprozess:

- **Vorbereitung:** SIM-Mitarbeiter nehmen laufend an Schulungen teil, damit sie reagieren können, wenn ein Sicherheitsvorfall auftritt.
- **Identifizierung:** Die Suche nach der Ursache eines Vorfalls, sei sie gezielt oder nicht, umfasst häufig die Verfolgung des Problems durch mehrere Ebenen der Microsoft Cloud Computing-Umgebung. Das SIM-Team wirkt bei der Ursprungsdiagnose für einen bestimmten Sicherheitsvorfall mit Mitgliedern anderer interner Microsoft-Teams zusammen.
- **Eingrenzung:** Nachdem die Ursache des Vorfalls festgestellt wurde, arbeitet das SIM-Team zusammen mit allen erforderlichen Teams an der Eingrenzung des Vorfalls. Welche Maßnahmen ergriffen werden, hängt von den Geschäftsauswirkungen des Vorfalls ab.
- **Minderung:** Das SIM-Team spricht sich mit relevanten Produkt- und Dienstbereitstellungsteams ab, um das Risiko eines erneuten Auftretens des Vorfalls zu mindern.
- **Wiederherstellung:** Durch weitere Zusammenarbeit mit anderen Gruppen ist das SIM-Team beim Wiederherstellungsprozess behilflich.
- **Erkenntnisse:** Nach der Problembehebung für den Sicherheitsvorfall beruft das SIM-Team eine gemeinsame Besprechung mit allen beteiligten Mitarbeitern ein, um die Geschehnisse zu bewerten und die während der Reaktion auf den Vorfall erworbenen Erkenntnisse aufzuzeichnen.

Das SIM-Team ist dank teamübergreifender Allianzen in der Lage, Probleme früh zu erkennen und Dienstauffälle zu mindern. Beispielsweise arbeitet das SIM-Team eng mit Betriebsteams zusammen, darunter dem Microsoft Security Response Center (weitere Informationen finden Sie auf der [Microsoft Security Response Center-Webseite](#)). Aufgrund dieser Beziehungen kann sich das SIM-Team schnell einen betrieblichen Gesamtüberblick über einen aktuellen Vorfall verschaffen. Der Antwortdienst des SIM-Teams berät sich dazu mit den Service Managern, um die Schwere des Vorfalls anhand einer Reihe von Faktoren zu bestimmen, darunter potenzielle oder zusätzliche Dienstauffälle und das Risiko einer Rufschädigung.

Global Criminal Compliance

Innerhalb des GCC-Programms (Global Criminal Compliance) von OSSC werden Richtlinien aufgestellt und Schulungen zum Reaktionsprozess von Microsoft angeboten. GCC stellt im gesetzlich vorgeschriebenen Rahmen bei Anforderung Informationen bereit. GCC verfügt in vielen Ländern über Rechtsberater, die etwaige Anfragen bewerten und bei Bedarf

übersetzen. Ein Grund dafür, dass GCC von vielen internationalen Behörden als ein „Programm mit hervorragender Reaktionsfähigkeit“ angesehen wird, liegt darin, dass GCC ein Portal für die Strafverfolgungsbehörden umfasst, das Anleitungen in mehreren Sprachen dazu enthält, wie befugte Behördenmitarbeiter eine rechtliche Anfrage bei Microsoft einreichen können.

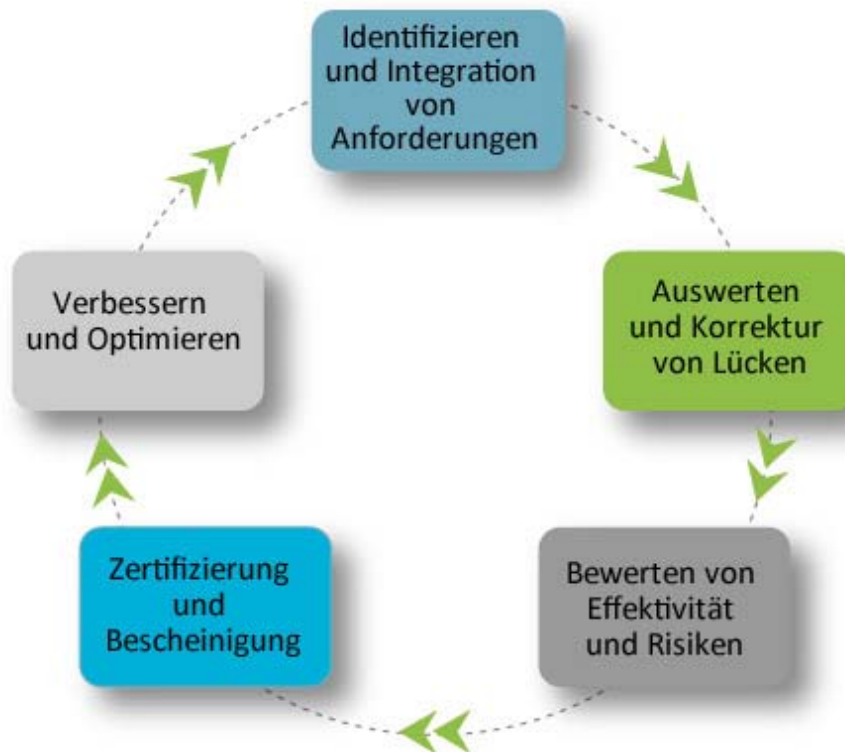
Zum Schulungsprogramm von GCC gehört auch die Schulung von Experten im Bereich Strafverfolgung. GCC bietet dazu Schulungen für Mitarbeiter aller Ebenen bei Microsoft zu den Themen Datenaufbewahrung und Datenschutz. Die internen Schulungsmaßnahmen und Richtlinien werden ständig weiterentwickelt, da Microsoft immer mehr Rechenzentren an internationalen Standorten einrichtet, sodass eine größere Anzahl internationaler behördlicher Vorschriften berücksichtigt werden müssen. GCC spielt eine entscheidende Rolle beim Verständnis und der Implementierung von Prozessen, die unterschiedlichen internationalen Gesetzen unterliegen, sowie bei der Anwendung dieser Gesetze auf Privat- oder Geschäftskunden, die sich auf Microsoft Online Services verlassen.

Betriebliche Compliance

Die Microsoft Online Services-Umgebung muss zusätzlich zu den Unternehmensspezifikationen von Microsoft eine Vielzahl behördlicher und branchenspezifischer Sicherheitsanforderungen erfüllen. Im Zuge des Wachstums und der Veränderungen bei Microsoft Online-Unternehmen werden neue Online Services in die Microsoft-Cloud aufgenommen, sodass zusätzliche Anforderungen aufgestellt werden, beispielsweise regionale und länderspezifische Datensicherheitsstandards. Das Operational Compliance-Team arbeitet mit den Betriebs-, Produkt- und Dienstbereitstellungsteams sowie mit internen und externen Prüfern zusammen, um sicherzustellen, dass Microsoft alle relevanten Standards und behördlichen Auflagen erfüllt. Die folgende Liste enthält eine Übersicht einiger Prüfungen und Bewertungen, die regelmäßig für die Microsoft Cloud-Umgebung durchgeführt werden:

- **PCI-Standard (Payment Card Industry) für Datensicherheit:** Jährliche Überprüfung und Validierung von Sicherheitskontrollen bei Kreditkartentransaktionen
- **Media Rating Council:** Integritätsüberprüfung der Datenerzeugung und -verarbeitung in der Werbebranche
- **Sarbanes-Oxley:** Jährliche Überprüfung bestimmter Systeme zur Bewertung der Einhaltung wichtiger Prozesse im Bereich Finanzberichte
- **HIPAA (Health Insurance Portability and Accountability Act in den USA):** Richtlinien zu Datenschutz, Datensicherheit und Notfallwiederherstellung bei der elektronischen Speicherung von Krankheitsdaten
- **Interne Prüfungen und Bewertungen zum Datenschutz:** Bewertungen über ein bestimmtes Jahr hinweg

Es war eine beachtliche Herausforderung für Microsoft, alle diese Prüfaufgaben zu erfüllen. Nach Untersuchung der Anforderungen kam Microsoft zu dem Schluss, dass bei vielen der Prüfungen und Bewertungen die gleichen Betriebsabläufe und -prozesse ausgewertet wurden. Microsoft erkannte die Chance, eine Vielzahl redundanter Arbeitsabläufe zu eliminieren, die Prozesse zu optimieren und die Richtlinieneinhaltung proaktiv und umfassender verwalten zu können. OSCC entwickelte daher ein umfassendes Compliance Framework. Dieses Framework und die damit verbundenen Prozesse basieren auf der in der folgenden Abbildung gezeigten Fünf-Stufen-Methode:



- **Identifizierung und Integration von Anforderungen:** Umfang und anwendbare Kontrollen werden festgelegt. Betriebliche Standardverfahren und Prozessdokumente werden gesammelt und überprüft.
- **Auswertung und Korrektur von Lücken:** Lücken bei Prozessen oder Technologie werden identifiziert und behoben.
- **Bewertung der Effektivität und Risiken:** Die Effektivität von Kontrollen wird gemessen und aufgezeichnet.
- **Zertifizierung und Bescheinigung:** Es findet eine Einbindung mit Zertifizierungsstellen von Drittanbietern und Prüfern statt.
- **Verbesserung und Optimierung:** Wenn die Nichteinhaltung von Vorschriften festgestellt wird, wird die Ursache dokumentiert und weiter untersucht. Alle Erkenntnisse werden so lange verfolgt, bis die Ursachen vollkommen behoben sind. Zu dieser Phase gehört auch das Optimieren von Kontrollen in allen Sicherheitsdomänen, um zukünftige Betriebs- und Zertifizierungsprüfungen effizienter zu gestalten.

Einer der Erfolge bei der Einführung dieses Programms ist es, dass die Cloud-Infrastruktur von Microsoft nach SAS 70 Typ I und Typ II bescheinigt und nach ISO/IEC 27001:2005 zertifiziert ist. Diese Erfolge zeugen aus den folgenden Gründen vom Engagement des Unternehmens Microsoft bei der Bereitstellung einer zuverlässigen Cloud Computing-Infrastruktur:

- Mit dem ISO/IEC 27001:2005-Zertifikat wird bescheinigt, dass Microsoft die in diesem Standard festgelegten international anerkannten Kontrollen zur Datensicherheit implementiert hat
- Die SAS 70-Bescheinigung zeugt von der Bereitwilligkeit von Microsoft, internationale Sicherheitsprogramme für externe Prüfungen offenzulegen.

Mehrstufige Abwehrstrategie

Die mehrstufige Strategie einer umfassenden Abwehr ist für Microsoft ein wichtiges Element einer zuverlässigen Cloud-Infrastruktur. Bei Kontrollen auf mehreren Ebenen sind Schutzmechanismen sowie das Entwickeln von Strategien zur Risikominderung erforderlich. Außerdem muss eine sofortige Reaktion auf Angriffe möglich sein. Der Einsatz mehrerer Sicherheitsmaßnahmen mit unterschiedlichen Stärken, je nach Wichtigkeit der geschützten Ressource, führt zu verbesserten Fähigkeiten beim Verhindern von Sicherheitsverletzungen oder zur Verringerung der Auswirkungen eines Sicherheitsvorfalls. Durch Cloud Computing ändert sich dieses Prinzip nicht, die Kontrollstärke hängt also weiterhin von der Wichtigkeit der Ressource ab. Außerdem ist das Prinzip nach wie vor für den Umgang mit Sicherheitsrisiken enorm wichtig. Die Tatsache, dass die meisten Ressourcen in einer Cloud Computing-Umgebung virtualisiert werden können, führt zu Veränderungen bei der Risikoanalyse sowie beim Einsatz von Sicherheitskontrollen auf herkömmliche tiefgreifende Schichten (physisches Netzwerk, Daten, Identitätszugriff, Zugriffsautorisierung und -authentifizierung und Hosts).

Online Services, darunter die Infrastruktur- und Plattformdienste von GFS, nutzen die Vorteile der Virtualisierung. Daher verfügen Kunden, die in der Microsoft-Cloud gehostete Dienste verwenden, möglicherweise über Ressourcen, die nicht mehr auf einfache Weise einer physischen Präsenz zugeordnet werden können. Daten können virtuell gespeichert und an viele Standorte verteilt werden. Diese grundlegende Tatsache bedeutet, dass Sicherheitskontrollen identifiziert werden müssen. Weiterhin muss ihr Einsatz zur Implementierung eines mehrschichtigen Ansatzes zum Schutz von Ressourcen bestimmt werden. Natürlich müssen auch weiterhin physische und Netzwerk-Sicherheitsmaßnahmen getroffen werden. Der Fokus beim Risikomanagement verschiebt sich jedoch näher an die Objektebene heran, näher an die Elemente, die in der Cloud-Umgebung verwendet werden. Dazu gehören beispielsweise die statischen oder dynamischen Container zur Datenspeicherung, die Laufzeitumgebungen, in denen Rechenvorgänge durchgeführt werden.

Bei den verschiedenen vorhandenen Kontrollen werden viele herkömmliche physische und Netzwerksicherheitsmethoden und -geräte verwendet. So wird sichergestellt, dass die Entität authentisch und für die Zugriffsanforderung autorisiert ist, ganz gleich, ob es sich um eine Person handelt, die Zugriff auf ein Rechenzentrumsgebäude erhalten möchte, oder um einen Rechenprozess, der Zugriff auf die dynamisch in der Microsoft Cloud-Umgebung gespeicherten Daten anfordert. Anhand weiterer integrierter Maßnahmen wird sichergestellt, dass die Server- und Betriebssysteminstanzen auf der Microsoft Cloud-Infrastruktur gegen Angriffe abgesichert sind.

In diesem Abschnitt erhalten Sie einen Überblick über einige der Prozesse und Kontrollen, die Microsoft zur Sicherheit von Rechenzentren, der Netzwerkhardware, der Netzwerkkommunikation und der Diensthosts verwendet.

Physische Sicherheit

Der Einsatz technischer Systeme zur automatisierten Zugriffsautorisierung und zur Authentifizierung für bestimmte Schutzvorrichtungen ist eine Methode, die dank der Weiterentwicklung von Sicherheitstechnologien zur physischen Sicherheit beiträgt. Eine weitere Veränderung bringt der Wandel von herkömmlichen Unternehmensanwendungen mit sich, die auf Computerhardware ausgeführt wurden, sowie physisch im Unternehmen vorhandener Software hin zu Software as a Service und Software plus Service. Aufgrund dieser Veränderungen müssen Unternehmen zusätzliche Maßnahmen ergreifen, um den Schutz ihrer Ressourcen zu gewährleisten.

OSSC übernimmt die physische Sicherheit für alle Rechenzentren von Microsoft. Diese Sicherheit ist für den kontinuierlichen Betrieb und den Schutz von Kundendaten unerlässlich. In jedem Rechenzentrum werden bewährte und präzise Verfahren für Sicherheitsentwürfe und Sicherheitsabläufe befolgt. Microsoft gewährleistet, dass äußere und innere Sicherheitsbereiche vorhanden sind, deren Kontrollen sich mit jeder Schicht erhöhen.

Im Sicherheitssystem werden eine Vielzahl von Technologielösungen gemeinsam eingesetzt, darunter Kameras, Biometrie, Kartenleser und Alarmer mit herkömmlichen Sicherheitsmaßnahmen wie Sperren und Schlüsseln. Darüber hinaus enthält es Funktionen zur Kontrolle über Betriebsabläufe, die die automatisierte Überwachung erleichtern und eine frühe Benachrichtigung im Falle einer Sicherheitsverletzung oder eines Problems gewährleisten. Durch die Bereitstellung einer prüffähigen Dokumentation zum Programm für die physische Sicherheit des Rechenzentrums wird zudem die Zuverlässigkeit sichergestellt. Die folgende Liste enthält weitere Beispiele zu den Sicherheitsmaßnahmen von Microsoft zur Gewährleistung der physischen Sicherheit:

- **Kriterien zur Einstellung von Rechenzentrumsmitarbeitern:** Microsoft stellt Sicherheitsanforderungen, anhand derer Rechenzentrumsmitarbeiter und Auftragnehmer überprüft werden müssen. Neben den Vertragsbestimmungen für interne Mitarbeiter gilt eine zusätzliche Sicherheitsebene für die Rechenzentrumsmitarbeiter, die für den Betrieb der Einrichtung zuständig sind. Der Zugriff wird durch das Prinzip der geringsten Berechtigung geregelt. So kann gewährleistet werden, dass nur ausgewählte Mitarbeiter Anwendungen und Dienste von Kunden verwalten.
- **Erfüllung von Anforderungen für Daten mit umfangreichen Geschäftsauswirkungen:** Für Rechenzentren, die Online Services anbieten, hat Microsoft strengere Mindestanforderungen für hochsensible Bestände definiert, die über die Anforderungen für nicht oder weniger sensible Bestände hinausgehen. In den Standardsicherheitsprotokollen für die Identifizierung, die Zugriffstoken und die Protokollierung und Überwachung von Sitezugriffen sind die erforderlichen Authentifizierungstypen klar angegeben. Für den Zugriff auf hochsensible Bereiche ist die mehrstufige Authentifizierung erforderlich.
- **Zentralisierung der Zugriffsverwaltung für physische Anlagen:** Mit der zunehmenden Anzahl von Rechenzentren, die Online Services bereitstellen, hat Microsoft ein Tool zur Verwaltung der Zugriffsteuerung auf physische Anlagen entwickelt. Durch die Zentralisierung des Workflows für die Anforderung, Genehmigung und Gewährung des Zugriffs auf Rechenzentren stellt dieses Tool zudem prüffähige Datensätze zur Verfügung. Das Tool arbeitet nach dem Prinzip der geringsten Berechtigungen und verfügt über einen integrierten Workflow für die Erlangung von Genehmigungen von verschiedenen Autorisierungsstellen. Es lässt sich an die Bedingungen vor Ort anpassen und ermöglicht den effizienteren Zugriff auf Verlaufsdaten für die Berichterstattung und die Einhaltung von Prüfvorschriften.

Netzwerksicherheit

Microsoft wendet nach Bedarf vielschichtige Sicherheitsebenen auf Rechenzentrumsgeräte und Netzwerkverbindungen an. Sicherheitskontrollen finden zum Beispiel sowohl auf Steuerungs- als auch auf Verwaltungsebene statt. Spezialisierte Hardware wie Lastenausgleichsmodule, Firewalls und Eindringenschutzsysteme sind vorhanden, um auf volumebasierte Denial-of-Service-Angriffe zu reagieren. Bei Bedarf wenden die Netzwerkverwaltungsteams mehrstufige Zugriffssteuerungslisten (ACLs) auf segmentierte virtuelle LANs (VLAN) und Anwendungen an. Über Gatewayfunktionen in der Netzwerkhardware kann Microsoft umfassende Paketüberprüfungen durchführen und im Falle von verdächtigem Netzwerkverkehr Warnmeldungen senden oder diesen vollständig blockieren.

Für die Microsoft Cloud-Umgebung ist eine globale, redundante interne und externe DNS-Infrastruktur vorhanden. Die Redundanz, die eine Fehlertoleranz ermöglicht, wird durch das Clustern von DNS-Servern erzielt. Dank zusätzlicher Kontrollsysteme können Denial-of-Service-Angriffe und schadhafte Cache-Angriffe verhindert werden. So wird zum Beispiel der Schreibzugriff auf DNS-Datensätze durch Zugriffssteuerungslisten (ACLs) innerhalb von DNS-Servern und DNS-Zonen auf autorisierte Mitarbeiter beschränkt. Alle DNS-Server verfügen über neue Sicherheitsfunktionen (z. B. die zufällige Anordnung von Abfragebezeichnern) der neuesten, sicheren DNS-Software. Die DNS-Cluster werden fortlaufend auf nicht autorisierte Software und Konfigurationsänderungen der DNS-Zonen sowie auf weitere schädliche Dienstereignisse geprüft.

DNS ist Teil des global vernetzten Internets. Für die Bereitstellung dieses Diensts ist die Zusammenarbeit vieler Organisationen notwendig. Microsoft engagiert sich in vielen dieser Organisationen, z. B. im DNS Operations Analysis and Research Consortium (DNS-OARC), in dem DNS-Experten aus der ganzen Welt vertreten sind.

Datensicherheit

Microsoft teilt Bestände in verschiedene Kategorien ein, denen unterschiedliche Sicherheitsstufen und Sicherheitsmaßnahmen zugeordnet werden. Die Kategorien berücksichtigen die relative Gefahr finanzieller oder rufschädigender Auswirkungen im Falle eines Sicherheitsvorfalls in der entsprechenden Kategorie. Nach der Klassifizierung eines Bestands werden die notwendigen Schutzmaßnahmen mithilfe der Strategie einer umfassenden Abwehr von Risiken festgelegt. Datenbestände, die beispielsweise als Bestand mit mittlerer Auswirkung kategorisiert werden, unterliegen Verschlüsselungsanforderungen, wenn sie auf Wechseldatenträgern gespeichert oder auf externe Netzwerke übertragen werden. Vertrauliche Daten müssen neben diesen Anforderungen auch Verschlüsselungsanforderungen für die Speicherung auf internen Systemen und Netzwerkübertragungen erfüllen.

Alle Microsoft-Produkte müssen den kryptografischen Standards des Security Development Lifecycle (SDL) entsprechen, in dem akzeptable und inakzeptable Kryptografie-Algorithmen aufgeführt sind. Schlüssel, die länger als 128 Bit sind, müssen beispielsweise symmetrisch verschlüsselt werden. Für asymmetrische Algorithmen gilt eine Mindestlänge der Schlüssel von 2.048 Bit.

Identitäts- und Zugriffsverwaltung

Microsoft regelt den Zugriff auf Bestände mit dem Prinzip der geringsten Berechtigung und auf „Need-to-know“-Basis (Angestellte erhalten nur so viele vertrauliche Informationen wie unbedingt notwendig). Wo immer möglich wird statt des individuellen Zugriffs die rollenbasierte Zugriffskontrolle für den logischen Zugriff auf bestimmte Arbeitsfunktionen oder Verantwortungsbereiche gewählt. Laut diesen Richtlinien wird der Zugriff verweigert, außer wenn der Daten-Inhaber diesen explizit gewährt.

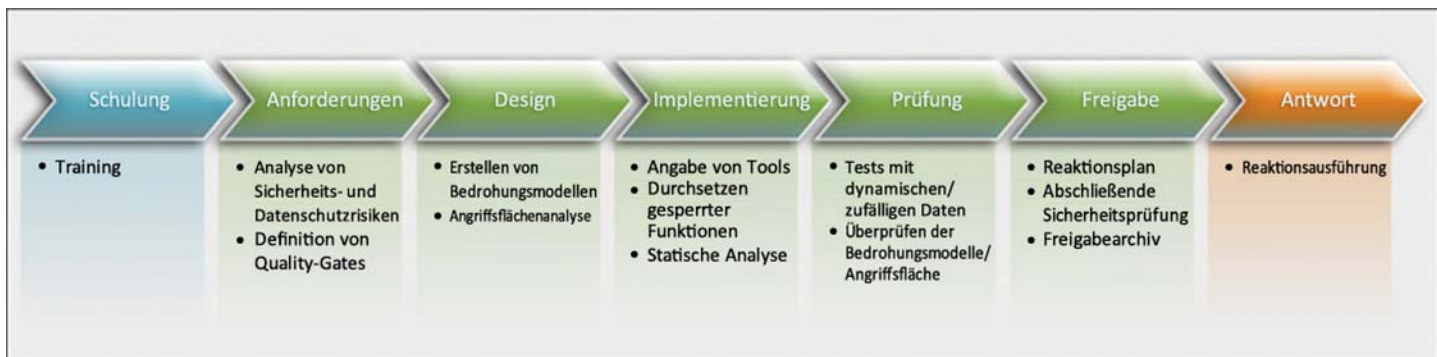
Personen, die für den Zugriff auf alle Bestände autorisiert sind, müssen die vorgeschriebenen Mittel für den Zugriff verwenden. Hochsensible Bestände erfordern eine mehrstufige Authentifizierung. Dazu zählen Maßnahmen wie Kennwörter, Hardwaretoken, Smartcards oder biometrische Daten. Die Abstimmung von Konten anhand von Autorisierungen für die Verwendung ist ein kontinuierlicher Prozess, mit dem sichergestellt wird, dass die Verwendung eines Bestands angemessen und für die Ausführung einer bestimmten Aktivität erforderlich ist. Konten, die nicht mehr für den Zugriff auf einen bestimmten Bestand benötigt werden, werden deaktiviert.

Anwendungssicherheit

Die Anwendungssicherheit ist eine der wichtigsten Komponenten für den Schutz der Cloud Computing-Umgebung von Microsoft. Die von den Entwicklungsteams bei Microsoft angewandten strengen Sicherheitspraktiken wurden 2004 im so genannten Security Development Lifecycle (SDL) veröffentlicht. Der SDL-Prozess ist eine agnostische Entwicklungsmethodik, die vollständig in den Anwendungsentwicklungszyklus integriert ist – vom Entwurf bis zur Nutzung. Er ist eine Ergänzung für andere Methodiken wie die agile Softwareentwicklung oder das Wasserfallmodell. Einige Phasen des SDL-Prozesses erfordern Schulungen und Weiterbildungen. Zudem müssen in jeder Phase der Softwareentwicklung die entsprechenden Aktivitäten und Prozesse eingehalten werden.

Führungskräfte von Microsoft sprechen sich weiterhin dafür aus, den SDL bei der Entwicklung von Microsoft-Produkten anzuwenden, einschließlich der Bereitstellung von Online Services. OSSC spielt eine entscheidende Rolle bei der Sicherstellung, dass der SDL-Prozess bei der aktuellen und zukünftigen Entwicklung von in der Microsoft Cloud-Infrastruktur gehosteten Anwendungen eingehalten wird.

Der SDL-Prozess wird in der folgenden Abbildung verdeutlicht:



Der SDL-Prozess umfasst mehrere spezifische Aktivitäten für die Entwicklung von Anwendungen, die in der Microsoft-Cloud gehostet werden sollen. Die erste Phase ist die Anforderungsphase.

- **Anforderungen:** Das Hauptziel dieser Phase besteht darin, die wichtigsten Sicherheitsziele zu identifizieren. Zudem soll die Softwaresicherheit maximiert und die Beeinträchtigung der Benutzerfreundlichkeit und der Pläne und Zeitpläne minimiert werden. Bei gehosteten Anwendungen kann für diese Aktivität eine Diskussion der betrieblichen Abläufe erforderlich sein, die sich darauf konzentriert zu definieren, auf welche Weise der Dienst Netzwerkverbindungen und Transportmechanismen für Nachrichten nutzt.
- **Design:** Zu den wichtigen Schritten in dieser Phase gehören die Dokumentierung der potentiellen Angriffsfläche und das Erstellen von Bedrohungsmodellen. Ähnlich wie bei der Definition der Anforderungen können auch hier Umgebungskriterien herausgearbeitet werden, wenn dieser Vorgang für eine gehostete Anwendung ausgeführt wird.
- **Implementierung:** Diese Phase besteht aus dem Erstellen und Testen des Codes. Zu verhindern, dass der erstellte Code Sicherheitslücken enthält, und diese ggf. zu entfernen, hat während der Implementierung oberste Priorität.
- **Überprüfung:** Anwendungen haben die Betaphase erreicht, wenn sie in ihrer Funktionalität vollständig sind. In dieser Phase liegt der Hauptaugenmerk darauf zu ermitteln, welche Sicherheitsrisiken bei Einsatz der Anwendung unter realen Bedingungen auftreten und welche Schritte zu deren Behebung bzw. Minderung unternommen werden können.
- **Veröffentlichung:** Die abschließende Sicherheitsprüfung Final Security Review (FSR) findet in dieser Phase statt. Bei Bedarf wird zusätzlich eine betriebliche Sicherheitsprüfung Operational Security Review (OSR) vorgenommen, bevor die neue Anwendung in der Cloud-Umgebung von Microsoft veröffentlicht wird.
- **Reaktion:** Für die Cloud-Umgebung von Microsoft übernimmt das SIM-Team die führende Rolle bei der Reaktion auf sicherheitsrelevante Vorfälle und kooperiert dabei eng mit Produkt- und Dienstbereitstellungsteams und Mitarbeitern des Microsoft Security Response Center, um gemeldete Vorfälle zu selektieren, zu untersuchen und zu beheben.

Weitere Informationen zum SDL finden Sie auf der [Microsoft Security Development Lifecycle \(SDL\)](#)-Seite.

OSSC übernimmt die Ausführung des FSR-Prozesses, eine SDL-Prüfung, die für Microsoft Online Services vorgeschrieben ist und gewährleistet, dass die entsprechenden Sicherheitsanforderungen erfüllt worden sind, bevor neue Anwendungen in der Cloud-Infrastruktur von Microsoft bereitgestellt werden. Bei der FSR wird überprüft, inwieweit die Prinzipien des SDL während des Entwicklungsvorgangs eingehalten wurden. OSSC führt dabei im Einzelnen folgende Aufgaben aus:

- **Koordinierung des Produktteams:** Fragebögen und andere Dokumente müssen vom Produktentwicklungsteam ausgefüllt werden. Anhand dieser Informationen wird überprüft, ob der SDL während der Produktentwicklung korrekt angewendet wurde.
- **Prüfung des Bedrohungsmodells:** Microsoft misst Bedrohungsmodellen für die Entwicklung von sicherer Software einen hohen Stellenwert bei. OSSC überprüft die von den Produktteams erstellten Bedrohungsmodelle auf Vollständigkeit und Aktualität. Des Weiteren wird in diesem Schritt geprüft, ob entsprechende Verfahren zur Beseitigung bzw. Minderung aller identifizierten Risiken implementiert wurden.
- **Prüfung von sicherheitsrelevanten Fehlern:** Sämtliche während Design, Entwicklung und Tests entdeckten Fehler werden überprüft, um sicherzustellen, dass Fehler behoben werden, welche die Sicherheit oder den Schutz von Kundendaten beeinträchtigen.
- **Prüfung der Toolverwendung:** Entwicklungs- und Testteams von Microsoft nutzen für den Entwicklungsprozess Softwaresicherheitstools sowie dokumentierte Codemuster und Praktiken. Diese Vorgehensweise führt durch die Vermeidung der häufigsten Sicherheitsschwachstellen zu einer erheblichen Verbesserung der Softwaresicherheit. OSSC stellt sicher, dass die Tools, der dokumentierte Code, die Muster und Praktiken vorschriftsmäßig und in geeigneter Weise von den Produktteams angewendet wurden.

Zusätzlich zum FSR-Prozess übernimmt OSSC auch die Durchführung der so genannten betrieblichen Sicherheitsprüfung (OSR). Die OSR besteht in der Prüfung der zugehörigen Netzwerkverbindungen, der Plattform und der Systemkonfiguration sowie der Überwachungsfunktionen anhand etablierter Sicherheitsstandards und -baselines. Sie stellt sicher, dass die betrieblichen Ablaufpläne angemessene Sicherheitskontrollen vorsehen, bevor eine Erlaubnis zur Bereitstellung in der Cloud-Infrastruktur gegeben wird.

Überwachung der Hostsicherheit und Berichterstellung

Um zuverlässige, gut organisierte, sichere und gepatchte Dienste anbieten zu können, muss eine in Umfang und Komplexität anwachsende Umgebung entsprechend verwaltet werden.

Das tägliche Scannen der Infrastrukturressourcen ermöglicht eine stets aktuelle Übersicht über die Schwachstellen der Hostsysteme und ermöglicht es OSSC, auftretenden Risiken in Kooperation mit den Produkt- und Dienstbereitstellungsteams entgegenzuwirken, ohne dabei den Betrieb der Microsoft Online Services übermäßig zu beeinträchtigen.

Die intern und extern ausgeführten Penetrationstests liefern wichtige Erkenntnisse über die Effektivität der Sicherheitskontrollen für die Cloud-Infrastruktur von Microsoft. Die Ergebnisse dieser Prüfungen und die kontinuierliche Bewertung der sich daraus ergebenden Kontrollen fließen in die nachfolgenden Scan-, Überwachungs- und Fehlerkorrekturmaßnahmen ein.

Durch die automatische Bereitstellung von standardmäßig abgesicherten Betriebssystem-Abbildern und aktive Kontrolle von Hostsicherheitsrichtlinien, z. B. der Gruppenrichtlinie, ist Microsoft in der Lage, die Aufnahme weiterer Server in seine Cloud-Infrastruktur zu steuern. Nach der Bereitstellung sorgen die betrieblichen Sicherheitsprüfungen und das Patchverwaltungsprogramm für eine kontinuierliche Risikominderung auf den Hostsystemen.

OSSC nutzt Überwachungs- und Berichterstellungsprozesse einerseits zur frühzeitigen Erkennung und Identifizierung von Bedrohungen, andererseits aber auch als Methode zur Gewinnung neuer Erkenntnisse und für die Sicherung „forensischer Beweise“ beim Auftreten eines Vorfalls. Die von Firewalls, Angriffserkennungssystemen und Netzwerkgeräten generierten Protokolle werden zentral im SYSLOG-Protokoll erfasst und in Dateiform gespeichert. Die einzelnen Ereignisdatensätze innerhalb dieser Dateien werden analysiert und in eine zentrale SQL Server-Datenbank hochgeladen. Die hochgeladenen Datensätze werden von automatischen Tools auf Muster untersucht, die auf anomales Verhalten oder böswillige Aktivitäten innerhalb der überwachten Umgebung schließen lassen, und lösen eine Alarmierung des SIM-Teams aus, sollte eine weitere Untersuchung der Aktivität erforderlich sein. Für jede der verarbeiteten Protokolldateien wird ein kryptografischer Hash erstellt und zusammen mit relevanten statistischen Angaben zur Datei in einer Datenbank gespeichert. Nach Generierung des Hashwerts werden die einzelnen Protokolldateien komprimiert und auf speziellen, redundanten Servern archiviert. Sollten die archivierten Originalprotokolldateien für zusätzliche Analysen benötigt werden, lässt sich ihre Integrität anhand des Hashwerts überprüfen.

Die Überwachungsprotokolle von kritischen Servern innerhalb der Cloud-Infrastruktur von Microsoft, also von Domänencontrollern, Sicherheitsservern und Servern, die vertrauliche Daten enthalten, werden nahezu in Echtzeit mithilfe der ACS-Funktion (Audit Collection Services) von Microsoft System Center Operations Manager erfasst und in einer SQL Server-Datenbank gespeichert. Aufgrund der umfangreichen Datenmengen, die für diese Umgebungen erfasst werden, werden wichtige und relevante Ereignisse (so genannte „Events-of-Interest“) extrahiert und in eine getrennte SQL-Datenbank hochgeladen, die dann von OSSC mithilfe automatisierter Tools eingehend auf verdächtige Aktivitäten untersucht wird. Zu den aus den Ereignisprotokollen erfassten Informationen gehören die Anmeldedaten des Benutzers, Änderungen an der Sicherheitsrichtlinienkonfiguration sowie der nicht-autorisierte Zugriff auf System- und Anwendungsdateien. Wie die von Firewalls und Netzwerkgeräten generierten Protokolle werden auch die aus den Überwachungsprotokollen extrahierten „Events-of-Interest“ auf Anzeichen von Versagen der Kontrollsysteme, das nicht autorisierte Modifizieren der Serverkonfiguration und weitere böswillige Aktivitäten untersucht.

Darüber hinaus sorgen benutzerdefinierte Management Packs, die für Microsoft Operations Manager (MOM) und Microsoft System Center Operations Manager erstellt werden, für Alarmgenerierung und Integritätsüberwachung in Echtzeit. Dies schafft zusätzliche Transparenz bei Sicherheitsverletzungen, Änderungen, welche die Systemintegrität gefährden, und Richtlinienverstößen auf einzelnen Systemen. Die Ereignisse aus Microsoft Operations Manager und System Center Operations Manager werden in die standardmäßigen Betriebsframeworks integriert und darüber hinaus intern bei Microsoft zur Behebung von weniger dringlichen Problemen genutzt.

Die aus den verschiedenen Protokolldateien extrahierten Informationen werden zur Generierung von Incidents, Berichten und historischen Trends verwendet, die wiederum für eine Tauglichkeitsprüfung der Mechanismen im Kontrollframework herangezogen werden.

Fazit

Auf Grundlage derselben Sicherheitsprinzipien, die auch bei der Handhabung von Risiken für die Softwareentwicklungs- und Betriebsumgebungen von Microsoft angewendet werden, hat OSSC ein Informationssicherheitsprogramm für Online Services erschaffen, das zu einer kontinuierlichen Verbesserung der Sicherheit für die Cloud Computing-Umgebung von Microsoft geführt hat. Dank eines koordinierten und strategisch ausgerichteten Einsatzes von Mitarbeitern, Prozessen und Technologien ist Microsoft in der Lage, auf kurzfristige Änderungen innerhalb der Cloud-Infrastruktur und am Markt für Online Services zu reagieren und gleichzeitig das Engagement des Unternehmens für die Bereitstellung von Trustworthy Computing für Kunden aufrecht zu erhalten.

Das Framework, mit dem Microsoft seine Zertifizierungen nach ISO 27001:2005 und SAS Typ I und Typ II erlangt hat, schafft die Voraussetzungen dafür, dass Produkt- und Dienstbereitstellungsteams bei Bedarf schneller zusätzliche Zertifizierungen und Bescheinigungen erhalten. Sicherheitsschulungen, die ständige Überprüfung von und der Umgang mit Sicherheitsrisiken, ein schnelles Reagieren auf sicherheitsrelevante Vorfälle und rechtliche Anfragen sowie die Tatsache, dass etablierte Verfahren hierfür bereits vorhanden sind, versetzen Microsoft in die Lage, sein Engagement für Trustworthy Computing aufrecht zu erhalten und gleichzeitig die Voraussetzungen dafür zu schaffen, dass auch Partner und Kunden von diesen ausgereiften und flexiblen Prozessen profitieren können.

Mit dem umfassenden Framework zu Compliance und den umfangreichen Kontrollmechanismen und -richtlinien, die durch das Informationssicherheitsprogramm bereitgestellt werden, bietet Microsoft seinen Kunden die Zuverlässigkeit und den Datenschutz, den sie erwarten können, und erfüllt gleichzeitig die behördlichen und gesetzlichen Auflagen sowie branchenübliche Standards. Die Erfolgsgeschichte von Microsoft und die unabhängig voneinander zertifizierten Programme des Unternehmens belegen die anhaltende Bedeutung dieser Programme für die Entwicklung von Herausforderungen und Chancen in dem sich fortwährend verändernden Markt für Online Services. Microsoft-Produktteams nutzen diese Praktiken im Rahmen der Software-plus-Services-Strategie für flexible und kosteneffektive Softwareentwicklung, um Vertrauen und ein angemessenes Maß an Transparenz zu schaffen. Das Vorhandensein einer vertrauenswürdigen Cloud-Infrastruktur versetzt Microsoft, Partner und Kunden in die Lage, Anwendungen für diese dynamische Cloud-Umgebung zu entwickeln, die mehr Sicherheit bieten.

Weitere Ressourcen

Microsoft Trustworthy Computing, Startseite: <http://www.microsoft.com/twc>

Microsoft Online Privacy Notice Highlights: <http://www.microsoft.com/privacy>

Das ISO 27001:2005-Zertifikat für die Global Foundation Services-Gruppe von Microsoft: <http://www.bsi-global.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search-Results/?pg=1&licencenumber=IS+533913&searchkey=companyXeqXmicrosoft>

Microsoft Global Foundation Services, Startseite: <http://www.globalfoundationservices.com>

Der Microsoft Security Development Lifecycle (SDL): <http://msdn.microsoft.com/en-us/security/cc448177.aspx>

Microsoft Security Development Lifecycle (SDL) – Version 3.2, Verfahrensinformationen: <http://msdn.microsoft.com/en-us/library/cc307748.aspx>

Microsoft Security Response Center: <http://www.microsoft.com/security/msrc>

Das Microsoft SDL-Tool zum Erstellen von Bedrohungsmodellen: <http://msdn.microsoft.com/en-us/security/dd206731.aspx>

Microsoft Online Services: <http://www.microsoft.com/online>

Bedingungen

Die Informationen in diesem Dokument geben die aktuelle Sichtweise der Microsoft Corporation hinsichtlich der erörterten Fragestellung zum Zeitpunkt der Veröffentlichung wieder. Da Microsoft auf sich ändernde Marktbedingungen reagieren muss, ist dieses Dokument nicht als unveränderlich zu betrachten. Microsoft übernimmt keine Garantie für die Genauigkeit der aufgeführten Informationen nach dem Veröffentlichungsdatum.

Dieses Whitepaper dient nur zu Informationszwecken. MICROSOFT SCHLIESST ALLE GARANTIEN, OB AUSDRÜCKLICH, KONKLUDENT ODER RECHTLICH, IN BEZUG AUF DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN AUS.

Der Benutzer ist verpflichtet, alle anwendbaren Urheberrechte einzuhalten. Ohne die Urheberrechte einzuschränken, darf kein Teil dieser Zusammenfassung für irgendwelche Zwecke vervielfältigt, auf einem Retrieval-System gespeichert, geladen oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufnehmen oder auf andere Weise) dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den Inhalt dieses Dokuments beziehen. Mit der Bereitstellung dieses Dokuments erhalten Sie keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird in einer schriftlichen Lizenzvereinbarung von Microsoft ausdrücklich vereinbart.

© 2009 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, Active Directory, Hotmail, Microsoft Dynamics, MSN, SharePoint, SQL Server, Windows Live und Xbox LIVE sind Marken der Microsoft-Unternehmensgruppe.

Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.