

Ein höheres Sicherheitsniveau durch Cloud-Lösungen

Das „Wer, Was, Wann, Warum und Wie“ cloudbasierter Sicherheitsdienste



Einleitung

Führungskräfte von heute wissen um die Bedeutung der Datensicherheit, haben jedoch immer wieder mit den Kosten und der Komplexität der Vielzahl an Sicherheitstechnologien zu kämpfen: Schutz vor Risiken, E-Mail-Sicherheit, Ermittlung von Sicherheitslücken und Verwaltung von Sicherheitsereignissen inklusive Protokolldatenmanagement. Während die Implementierung und Verwaltung dieser Lösungen auf der einen Seite für eine umfassende Sicherheitsstrategie von großer Bedeutung sind, führen sie auf der anderen Seite möglicherweise dazu, dass IT-Mitarbeiter nicht mehr gezielt für andere kritische Initiativen zur Verfügung stehen. Zudem können sich Unternehmen mit kleinerem Budget den Einsatz hoch entwickelter, komplexer Sicherheitslösungen („Defense-in-Depth“) möglicherweise nicht leisten. Cloud-Computing bietet ein Modell zur Bereitstellung der Sicherheitslösungen, mit dem viele dieser Herausforderungen in Unternehmen aller Größen adressiert werden.

Cloud-Computing ist eine flexible, kosteneffiziente und bewährte Plattform für die Bereitstellung von IT-Diensten für Unternehmen und Konsumenten über das Internet. Alle Prozesse, Anwendungen und Services werden bedarfsgerecht zur Verfügung gestellt. Daher können Cloud-Ressourcen schnell ausgerollt werden und sind einfach zu skalieren, und zwar unabhängig von Standort und System des Benutzers. Cloud-Computing hilft Unternehmen somit, die Servicebereitstellung effektiver zu gestalten, das IT-Management zu optimieren und die IT-Services besser auf dynamische Geschäftsanforderungen abzustimmen.

Im Bereich Datensicherheit bietet Cloud-Computing je nach vorhandener Sicherheitssoftware und den vorhandenen Systemen zahlreiche Vorteile. Cloudbasierte Sicherheitsdienste (auch bekannt als „Hosted Security“ oder „Security Software as a Service“) stellen Sicherheitsfunktionen über das Internet bereit. Der Kunde erwirbt keine Sicherheitsanwendungen, sondern abonniert vielmehr eine komplette Lösung, die remote zur Verfügung gestellt wird. Es müssen keine Hardware- bzw. Softwarelizenzen käuflich erworben werden und somit fallen auch keine damit einhergehenden Wartungsgebühren an. Das Cloud-Bereitstellungsmodell ermöglicht zudem eine Reduktion der Komplexität, da Unternehmen sich zukünftig nicht mehr mit Verwaltung, Konfiguration und Patches einer immer größer werdenden Anzahl an Sicherheitskomponenten und -technologien konfrontiert sehen. Der Einsatz von Sicherheitsdiensten über eine Cloud bietet Kunden in vielerlei

Hinsicht das Beste aus beiden Welten. Sie haben Zugang zu hoch entwickelten Sicherheitstechnologien sowie aktuellen sicherheitsspezifischen Informationen, und dies ohne durch interne Lösungen verursachte Kosten oder den zusätzlichen Aufwand oder die Verantwortung für das Management.

Die Fragen nach dem „Wer, Was, Wann, Wo, Warum und Wie“ cloudbasierter Sicherheitsdienste zeigen, wie mehr Sicherheit ohne großen finanziellen Aufwand dazu beitragen kann, Risiken zu minimieren, Ressourcen zu optimieren, mehr Flexibilität zu ermöglichen und gesetzliche Bestimmungen einzuhalten.

Wer profitiert von Sicherheitslösungen, die durch eine Cloud bereitgestellt werden?

Sicherheitsbedrohungen und Schwachstellen kennen keine vertikalen Grenzen zwischen den Branchen und Industrien und unterscheiden nicht zwischen kleinen und großen Unternehmen. Hoch entwickelte Sicherheitstechnologien sind in der Regel jedoch größeren Unternehmen vorbehalten, da diese über das notwendige Budget und Wissen für Installation, Management und Überwachung fortschrittlicher Unternehmenslösungen verfügen. Vielen Unternehmen fehlt es demnach an Schutz vor neuen Risiken – und zwar nicht absichtlich oder aus Nachlässigkeit, sondern aus Mangel an Ressourcen.

Cloudbasierte Sicherheitsdienste bieten Unternehmen aller Größen einen Mehrwert. Im Vergleich zu interner Sicherheitssoftware erfordert Cloud-Sicherheit wenige bis überhaupt keine Vorabinvestitionen und Implementierungskosten. Zudem ermöglicht das Cloud-Bereitstellungsmodell eine Reduzierung der laufenden Betriebskosten. Darüber hinaus werden branchenspezifische Anforderungen an das Risikomanagement erfüllt – für Behörden, den Handel oder für Fertigungsunternehmen.

Cloud-Sicherheitsdienste tragen nicht nur zur Reduzierung der Kosten und zur Erfüllung der Anforderungen an das Risikomanagement bei, sondern unterstützen auch Kunden mit begrenzten operationalen Ressourcen dabei verstärkt in strategische Initiativen zu investieren, die einen realen geschäftlichen Nutzen fördern. Im Vergleich zu traditionellen internen Sicherheitsimplementierungen verwenden Unternehmen, die sich für den Einsatz einer Cloud entschieden haben, weniger Zeit dafür, Systeme zu verwalten, technische Probleme zu beheben oder auf neueste Bedrohungen zu reagieren.

Was sind cloudbasierte Sicherheitsdienste?

Cloudbasierte Sicherheitsdienste werden remote – als externe Dienste – bereitgestellt und bieten Sicherheitsfunktionalitäten und sicherheitsspezifische Dienste durch einen Dienstleister. Sie verbinden Managed Services, Technologie und sicherheitsspezifische Dienste, um Sicherheitsfunktionen in bereits bestehenden Geschäftsprozesse zu integrieren, schützen vor Angriffen und Missbrauch, stellen sich den wichtigsten Anforderungen und werden Veränderungen gerecht. Mithilfe cloudbasierter Sicherheitsdienste können Kunden routinemäßige Sicherheitsaktivitäten effektiver und kosteneffizienter ausführen, indem sie die Technologie und Infrastruktur, die von vertrauenswürdigen Dritten bereitgestellt wird, nutzen. Dies hilft Kunden, Kosten durch eine flexible nutzungsorientierte Preisgestaltung einzusparen. Der Cloud-Sicherheitsdienstleister übernimmt die Verantwortung für Funktionalität, Implementierung, Leistung und Wartung der Anwendung und entlastet den Kunden somit von diesen aufwendigen Aktivitäten.

Cloudbasierte Sicherheitsdienste bieten gegenüber traditionellen Sicherheitsimplementierungen folgende Vorteile:

- Es muss keine kostenintensive, interne Sicherheitshardware erworben, installiert und gewartet werden.
- Es gibt keine separate Software, für die regelmäßig Updates und Patches zu installieren sind.
- Webbasierte Portale ermöglichen eine schnelle Implementierung und bieten Self-Service-Funktionen.
- Die Möglichkeit zur Skalierung und Erweiterung der Sicherheitsfunktionen, ohne dass dabei in zusätzliche Infrastruktur investiert werden muss.
- Eine flexible, dienstorientierte Preisgestaltung und Service-Level-Vereinbarungen werden ermöglicht.

Herkömmliche Sicherheitslösungsansätze erfordern den Kauf mehrerer Sicherheitstechnologien und Managementsysteme sowie einen höheren Personalbedarf für Integration, Konfiguration und Patching. Cloudbasierte Dienste ermöglichen eine Reduzierung dieser Ausgaben und bieten eine ideale Bereitstellungsmethode für zahlreiche externalisierte Sicherheitsfunktionen wie

- Ermittlung von Sicherheitslücken
- Web/URL-Filterung
- Management von Sicherheitsereignissen
- Management von Sicherheitsprotokollen
- E-Mail-Sicherheit

Neben der Sicherheitsfunktionalität stellen cloudbasierte Sicherheitsdienste zudem aktuelle sicherheitsspezifische Informationen und Analysen bereit, damit alle Sicherheitstechnologien immer auf dem aktuellen Stand bleiben. Ein Unternehmen, das beispielsweise vor drei Jahren ein E-Mail-Sicherheitssystem erworben hat, muss sich der Hausforderung stellen, diese möglicherweise immer wieder zu aktualisieren, um zu verhindern, dass das System den aktuellen Risiken nicht mehr gewachsen ist. Mithilfe cloudbasierter Sicherheitslösungen entwickelt sich der Dienst im Laufe der Zeit weiter und bleibt immer auf dem aktuellen Stand, indem die neuesten Funktionalitäten und Inhalte berücksichtigt werden.

Wann liefern cloudbasierte Sicherheitsdienste reale Vorteile?

Die Flexibilität cloudbasierter Sicherheitsdienste kann die Arbeitsweise in Unternehmen dadurch verändern, dass die Sicherheitslösung in einer nie da gewesenen Art und Weise auf zukünftige Geschäftsanforderungen abgestimmt wird. Die Vorteile der cloudbasierten Sicherheit zeigen sich immer dann ganz besonders, wenn Unternehmen einen Wandel erleben, der sie dazu veranlasst, das Thema Sicherheit erneut zu überdenken und die Prioritäten neu zu setzen. Ein Beispiel: Cloudbasierte Sicherheit bietet Sicherheit und Vorteile für Geschäftsprozesse, wenn es um neue gesetzliche Bestimmungen, Firmenübernahmen oder das Hinzufügen eines neuen Geschäftsbereichs bzw. neuer Systeme geht. Cloud-Sicherheitsdienste arbeiten in solchen Fällen problemlos in einer sich wandelnden IT-Umgebung, ohne dass der Kunde dafür Mitarbeiter aus den Bereichen für Informationstechnologie und Sicherheit von anderen kritischen Initiativen abziehen muss.

Wo arbeiten cloudbasierte Sicherheitsdienste am besten?

Cloud-Sicherheitsdienste bieten sich in allen Fällen an, in denen Unternehmen eine Verbindung zum Internet haben und Datenbestände schützen möchten. Egal ob weltweit, in der Unternehmenszentrale oder nur an fernen Standorten angewandt: Die Entscheidung wird durch die Geschäftsanforderungen bestimmt. Durch den Einsatz von Cloud-Sicherheitsdiensten müssen sich Unternehmen nicht zu einer umfangreichen Implementierung verpflichten. Sie können stattdessen das Bereitstellungsmodell testen, indem Sie es zunächst nur über gehostete Sicherheitsfunktionen für einen bestimmten Standort oder für ein bestimmtes Segment der IT-Infrastruktur anwenden, während sie andere Sicherheitsbereiche weiterhin intern verwalten. Unternehmen, die sich für Cloud-Sicherheitsdienste entscheiden, haben Zugang zu allen Funktionen des Sicherheitsdienstes, z. B. erweiterte Analysen und Korrelation, künstliche Intelligenz, branchenführendes Sicherheits-Know-how und ein webbasiertes Verwaltungsportal. Dies ist unabhängig davon, ob ein Unternehmen nur ein einzelnes Rechenzentrum oder eine komplette IT-Infrastruktur schützen möchte.

Warum benötigen Unternehmen cloudbasierte Sicherheitsdienste?

Cloud-Sicherheitsdienste stellen Schutzmaßnahmen auf eine einfachere, effizientere und kostengünstigere Art und Weise bereit, sodass Kunden sich auf ihre wichtigen Geschäftsbereiche fokussieren können. Das Bereitstellungsmodell für cloudbasierte Sicherheit ermöglicht eine Transformation des Sicherheitsansatzes im Unternehmen, indem sicherheitsrelevante Entscheidungen mehr denn je strategisch beschlossen werden und Sicherheitstechnologien auf die sich verändernden Geschäftsanforderungen abgestimmt werden. Mithilfe eines Sicherheitsportals, das die Darstellung der sicherheitsspezifischen Informationen sinnvoll integriert, können Kunden fundiertere Geschäftsentscheidungen treffen, wenn es darum geht, Risiken zu

minimieren. Der Anbieter eines Cloud-Sicherheitsdienstes übernimmt die komplexen und die alltäglichen Aufgaben, während der Kunde weiterhin die Kontrolle und die Verantwortung behält.

Durch die Cloud-Sicherheitsdienste profitieren die Kunden von einer konsolidierten Sicht auf die Sicherheitsinfrastruktur ihres Unternehmens durch das Sicherheitsportal zur Bereitstellung sicherheitsspezifischer Informationen. Daten zu Sicherheitsereignissen sind nur dann nützlich, wenn Unternehmen in der Lage sind, diese zu analysieren und gegebenenfalls Maßnahmen zur Problembehebung zu ergreifen. Eine durch die Cloud bereitgestellte konsolidierte Sicht der Sicherheitsinfrastruktur ermöglicht es Verantwortlichen, die Anzahl an aufgedeckten und beseitigten Schwachstellen sowie die Kosteneinsparungen, die durch einen besseren Datenverkehr und die effizientere Nutzung der Bandbreite erzielt wurden, zu berichten.

Die Flexibilität und Zuverlässigkeit eines Portals für cloudbasierte Sicherheitsdienste verbessert zudem die Einhaltung gesetzlicher Bestimmungen. Die für die Audits erforderlichen Informationen – Schwachstellen, Sicherheitsereignisse, Protokolldateien usw. – werden revisionsicher erfasst und verwaltet. Über das zentrale Portal sind die Informationen zur Überwachung und Prüfung schneller und einfacher verfügbar, da sie nicht von vielen verschiedenen Managementkonsolen separat abgerufen werden müssen.

Das cloudbasierte Bereitstellungsmodell nutzt bereits vorhandene IT-Investitionen wie Router, Anwendungsserver und Sicherheitssoftware. Cloudbasierte Sicherheitsdienste passen sich an Skalierungsfaktoren wie Größe, personelle Veränderungen sowie Veränderungen in der Geschäftstätigkeit an. Dieser Ansatz ermöglicht einen schnelleren Schutz, reduziert die erforderlichen internen Ressourcen, steigert die Rentabilität und legt den Fokus verstärkt auf die „Operational Excellence“.

Wie finden Sie den idealen Anbieter für cloudbasierte Sicherheitsdienste?

Ein effektiver Serviceanbieter verfügt über die perfekte Kombination aus Erfahrung im Bereich Servicebereitstellung, Managed Services, Technologie und Sicherheits-Know-how. Cloud-Sicherheitsdienste sollten von Sicherheitsexperten bereitgestellt werden, die Folgendes bieten:

- Bewährte Erfahrung in der Bereitstellung von Sicherheitsfunktionen über das Internet
- Ein zentrales Portal, das Kunden jederzeit einen Überblick über ihre Sicherheitsinfrastruktur ermöglicht
- Eine vollständig verwaltete Sicherheitsdienste-Plattform, einschließlich Gerätemanagement und cloudbasierter Sicherheitsdienste
- Eine komplette Sicherheitssuite für die gesamte IT-Infrastruktur
- Proaktive Sicherheitsinformationen in Echtzeit zum Schutz vor Risiken und zur Ermittlung von Schwachstellen
- Die Möglichkeit zur Nutzung der vorhandenen Infrastruktur und Sicherheitstechnologie
- Das Wissen um die Bedeutung von Risikomanagement für Geschäftsprozesse wie Anwendungsimplementierung, Compliance-Management, Supply-Chain-Management und vieles mehr
- Zuverlässig unterstützende Audit- und Compliancefunktionen, um Ihren Unternehmensanforderungen gerecht zu werden
- Eine globale Bereitstellung mit weltweiter geografischer Abdeckung und kontinuierlicher Verfügbarkeit

Cloudbasierte Sicherheitsdienste von IBM Managed Security Services

IBM ist seit der Konzeption von Cloud-Computing in diesem Bereich führend. Darüber hinaus ist IBM aufgrund seiner fast zehnjährigen Erfahrung mit diesem Bereitstellungsmodell ein bewährter Anbieter von Cloud-Sicherheitsdiensten. Als anerkannter Berater in Sicherheitsfragen für Tausende weltweit führende Unternehmen sowie staatliche Organisationen war IBM immer führend im Bereich vielfältiger Sicherheitstechnologien wie Schwachstellenanalyse, Virenschutz und präventiver Maßnahmen.

IBM war einer der Wegbereiter für die Bereitstellung des cloudbasierten Schwachstellenmanagements und der Verwaltung von Sicherheitsereignis- und Protokolldateien, sowie für die Bereitstellung webbasierter Kundenportale für zentrale cloudbasierte Sicherheitsdienste und des Sicherheitsgerätemanagements.

Das „IBM Virtual Security Operations Center Customer Portal“ (Virtual-SOC-Kundenportal) bietet den Kunden einen besseren Überblick sowie eine bessere Kontrolle über die gesamte Sicherheitsinfrastruktur. Kunden verwenden das Virtual-SOC-Portal als zentrale Befehls- und Steuerzentrale für alle ihre IBM Cloud-Sicherheitsdienste und Managed Security Services für das Gerätemanagement. Durch dieses sichere webbasierte Portal verfügen die Kunden über die notwendigen Informationen und Werkzeuge, um Entscheidungen in Echtzeit zu treffen und somit die Sicherheit verbessern zu können. Dieses mit vielen Funktionen ausgestattete Portal stellt Unternehmen eine Befehlszentrale für die Überwachung und Kontrolle der Sicherheitsoperationen im gesamten Unternehmen zur Verfügung. Das Virtual-SOC-Portal ist jederzeit und überall verfügbar und bietet das umfassende Wissen des IBM X-Force Security Intelligence-Teams, Dienste für die frühzeitige Risikoanalyse, ein individuell angepasstes Berichtswesen sowie die interaktiven Kommunikationsmöglichkeiten zwischen dem Kunden und dem Security Operations Center. Dies ermöglicht die Zusammenarbeit zwischen Kunden, Ihrem Unternehmen und den Sicherheitsexperten von IBM.

Die IBM Sicherheitsprodukte und -dienste basieren auf den proaktiven Sicherheitslösungen des X-Force Forschungs- und Entwicklungsteams – der weltweit führenden Organisation im Bereich Analyse und Bewertung von Schwachstellen und Risiken. Darüber hinaus verfügt IBM über das notwendige Wissen, Kunden und ihre bestehenden Geschäftsprozesse in der Integration der Themen Sicherheit und Risikominimierung zu unterstützen.

Cloudbasierte Sicherheitsdienste von IBM Managed Security Services umfassen:

- **Hosted Security Event and Log Management** – Ermöglicht die Erfassung von Ereignis- und Protokolldateien aus Netzwerkanwendungen, Betriebssystemen und anderen Sicherheitstechnologien in einer übergreifenden Plattform. Dies beinhaltet die Integration von Workflow- und Analysefunktionen sowie das reibungslose Speichern an einem externen Standort.
- **Hosted Vulnerability Management** – Kombiniert die zur Erkennung und Beseitigung von Sicherheitsproblemen verwendeten Managed Scanning Services mit dem Fachwissen zu Workflow- und Case-Management und unterstützt somit die Compliance.
- **Hosted Email and Web Security** – Bietet rund um die Uhr cloudbasierten Schutz vor Spam, Computerwürmern, Viren, Spyware, Adware und anzüglischen Inhalten.
- **IBM X-Force Hosted Threat Analysis Service** – Stellt individuell angepasste Sicherheitslösungen auf der Grundlage von sicherheitsspezifischen Informationen des X-Force Research and Development-Teams zur Verfügung.

Das Produktangebot cloudbasierter Sicherheitsdienste von IBM wird zudem durch ein umfassendes Portfolio herkömmlicher Lösungen für die Bereiche „Managed Security“ und „Professional Services“ ergänzt.

Weitere Informationen

Wenn Sie mehr über die cloudbasierten Sicherheitsdienste von IBM Managed Security Services erfahren möchten, wenden Sie sich an Ihren IBM Vertriebsbeauftragten oder IBM Business Partner oder besuchen Sie die folgende Website: ibm.com/services/us/index.wss/offerfamily/iss/at026954

Finanzierungslösungen von IBM Global Financing bieten Möglichkeiten wie effektive Finanzdisposition, Schutz vor überalterter Technologie, Reduzierung der Gesamtbetriebskosten und einen höheren Return-on-Investment. Zudem helfen unsere Global Asset Recovery Services dabei, durch neue energieeffizientere Lösungen auch dem Umweltschutz Rechnung zu tragen. Weitere Informationen zu IBM Global Financing finden Sie unter: ibm.com/financing



IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

IBM, das IBM Logo und ibm.com sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter:

ibm.com/legal/copytrade.shtml

Weitere Unternehmens-, Produkt- oder Servicennamen können Marken anderer Hersteller sein.

Der Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. Es obliegt allein dem Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Einhaltung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die sich auf seine Geschäftstätigkeit und alle Maßnahmen auswirken können, die er im Hinblick auf die Einhaltung solcher Bestimmungen durchführen muss.

IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit jeglichen relevanten Gesetzen und Verordnungen.

© Copyright IBM Corporation 2011
Alle Rechte vorbehalten.



Bitte der Wiederverwertung zuführen