

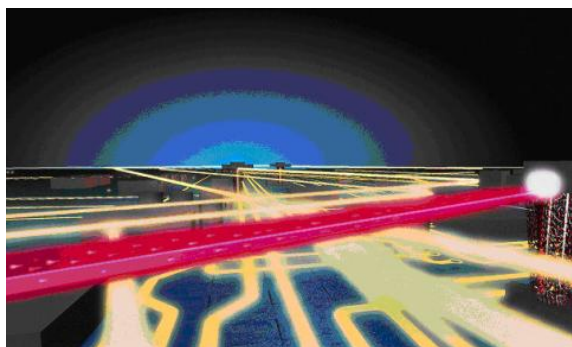
Security-Risiken beim Cloud Computing

› Viele IT-Manager schrecken aus Sorge um die Sicherheit und Verfügbarkeit von Anwendungen und Daten vor der Nutzung von Cloud-Computing-Diensten zurück. Doch die Security-Risiken lassen sich eindämmen.

Von Rene Reutter und Thorsten Zenker, T-Systems (02.10.2009 05:00:00)

Damit sie mit der Wolken-IT nicht plötzlich im Regen stehen, scheuen große Unternehmen nach einer aktuellen Studie der amerikanischen Information Technology Intelligence Corporation (ITIC) den Schritt zum [Cloud Computing](#)¹. Die Marktforscher befragten international 300 Firmen mit bis zu 100.000 Mitarbeitern. Lediglich 15 Prozent von ihnen wollen in absehbarer Zeit entsprechende Technologien einsetzen, nur acht Prozent tun es bereits. Die größten Ängste existieren hinsichtlich der [Sicherheit](#)²: Zum einen ist meist nicht genau bekannt, wo auf dem Erdball die sensiblen Daten gespeichert sind. Wie steht es da zum Beispiel mit der Compliance? Welchem Landesrecht unterliegen die Informationen? Zum anderen besteht die Sorge, dass das Geschäft durch einen längeren Netzausfall zum ruinösen Stillstand kommt.

Wie so oft entstehen Ängste durch Skepsis vor dem Neuen: Gerüchte kursieren und es herrscht mangelhafte Aufklärung. Wer aber weiß, welche Sicherheitslücken drohen und wie er sich schützen kann, muss sich weniger fürchten, denn die Risiken lassen sich auf ein Minimum reduzieren. Hier sind die [Cloud-Computing-Provider](#)³ in der Pflicht, ihre Kunden über die für sie am besten geeigneten Sicherheitsmaßnahmen zu informieren. Welche davon er nutzt, bleibt jedem Anwender dann selbst überlassen. Aber nur wer das persönliche Sicherheitsniveau richtig einschätzen kann, entdeckt für sein Geschäft in der Wolke mehr als ominösen Nebel.



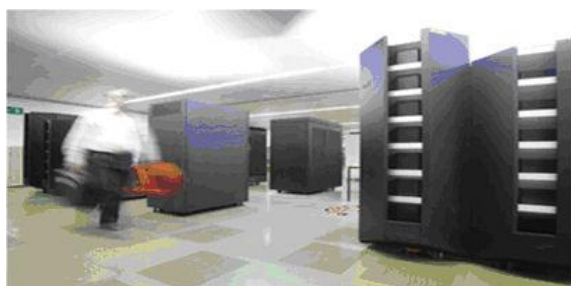
Cloud Computing in der Praxis: Nur wenige deutsche IT-Verantwortliche wollen derzeit Cloud-Services nutzen. Grund dafür sind oft Sicherheitsbedenken.



Security Konzepte in der Cloud: Auch in der Cloud beginnt ein Sicherheitskonzept mit einer gründlichen Gefahren- und Anforderungsanalyse.



Daten und Anwendungen in der Cloud: Daten und Anwendungen müssen im Rechenzentrum des Cloud-Providers sauber voneinander getrennt sein.



Datensicherheit im Zeitalter der Cloud: Cloud-Nutzer wissen in der Regel nicht, auf welchen Systemen, in welchem Rechenzentrum und in welchem Land der Provider ihre Daten speichert.



Cloud Computing Netzinfrastruktur: Das Rückgrat jeder Cloud bilden stabile, breitbandige Netze. Wie auch immer die Netzverbindung konkret realisiert wird, sie sollte genau wie beim normalen Outsourcing doppelt ausgelegt sein und über zwei voneinander getrennte physikalische Verbindungen laufen. Fällt dann eine der beiden Leitungen aus, kann die andere nahtlos den Dienst der anderen übernehmen.



Monitoring Systeme: Monitoring- und Frühwarnsysteme sorgen für mehr Sicherheit in der Cloud-Infrastruktur. Sie spüren beispielsweise auf der Basis von Data-Mining-Verfahren Schwachstellen auf, bevor diese sich gefährlich auswirken.



Sicherheit planen: Security beginnt in den Köpfen. Regelmäßige Workshops und Schulungen können die generelle Wachsamkeit im Umgang mit IT-Lösungen in der Cloud steigern.

» Privat versus öffentlich

Schon die von Anbieter zu Anbieter beziehungsweise Analyst zu Analyst unterschiedlichen Definition der **Cloud**⁴ führen zu gravierenden Missverständnissen: Meist geht es um ein Verlagern der ICT-Ressourcen von lokalen Rechnern ins öffentliche, unsichere Internet. Aber muss das zwangsläufig so sein? Hier gilt es, grundsätzlich zwischen öffentlichen ("public") Clouds à la **Amazon**⁵ und **Google**⁶ sowie dedizierten ("private") Clouds für Unternehmen zu unterscheiden. Erstere eignen sich primär für private Nutzer, um zum Beispiel Mails überall zu empfangen und zu versenden oder um Dateien und Urlaubsfotos bequem auf Festplatten im Netz abzulegen. Sie kosten meist nichts, ihre Betreiber verpflichten sich aber auch zu nichts. Bei einem Server-Ausfall müssen die Anwender eben warten. Geht ein Mailserver oder eine Festplatte kaputt, sind die Daten weg. Sicherheit und Servicevereinbarungen - Fehlanzeige.

No risk, no fun? Was sich im privaten Umfeld mehr und mehr durchsetzt, widerspricht deutlich den Anforderungen der Geschäftswelt. Von der **Datensicherheit**⁷, dem Schutz gegen Manipulationen und einer hohen Verfügbarkeit hängt oft das Überleben eines Unternehmens ab. Weltweit stünden die meisten Firmen nach gut einer Woche ohne ihre IT-Daten vor dem Ruin. Und neben einem hohen finanziellen Verlust leidet meist auch das Image, wenn Informationen über eine neue Produktentwicklung schon vor ihrer offiziellen Publikation nach außen dringen. Sollten Unternehmen also trotz der hohen Flexibilität und der rein verbrauchsabhängigen Bezahlung lieber auf die Wolke verzichten? Die Antwort liegt in der "privaten" Cloud, einem Kompromiss aus Wolke und eigener Anbindung an ein Data Center. Hier fließen die Daten nicht über das öffentliche Internet, sondern über das getunnelte Netz des Providers.

» 1. Dienstleister auswählen

Die wohl größte Herausforderung für Unternehmen beim **Cloud Computing**⁸ besteht darin, den geeigneten Dienstleister zu finden. Sie müssen sich hierzu intensiv mit den von ihm angebotenen Services und seiner tatsächlichen Leistungsfähigkeit befassen. Kann er zum Beispiel individuelle Bedürfnisse bedienen? Wie gut kennt er sich mit branchenspezifischen Anforderungen aus? Große ICT-Anbieter erbringen identische Leistungen für eine Vielzahl von Kunden. Durch die sich daraus ergebenden Skaleneffekte können sie Technologien einsetzen, die für ein einzelnes Unternehmen kaum erschwinglich wären. Es müsste darüber hinaus Personal mit den richtigen Fachkenntnissen vorhalten und das Wissen der Mitarbeiter regelmäßig in Schulungen aktualisieren. Über den Provider kaufen sie das Fach- und Branchen-Know-how gleich mit ein. Das macht sich insbesondere bei der **Sicherheit**⁹ schnell bezahlt. Die Angreifer kennen sich meist mit den neuesten Werkzeugen perfekt aus. Hier mitzuhalten, erfordert einen beträchtlichen finanziellen und personellen Aufwand.

» 2. Security-Anforderungen definieren

Gleichwohl sollten Unternehmen nicht sofort die ganze **Sicherheit**¹⁰ einfach auf den Provider schieben, sondern sich mit ihm zunächst intensiv über das nötige Schutzniveau auseinandersetzen. Der Dienstleister muss seinem Kunden die bestehenden Risiken erläutern und ihm sagen, was er konkret dagegen unternimmt. Erst aus einer gründlichen Gefahrenanalyse lässt sich eine individuelle Lösung ableiten, die sämtliche Sicherheitsanforderungen erfüllt.

Genau wie bei klassischen ICT-Umgebungen reicht beim Cloud Computing das punktuelle Stopfen von **Security**¹¹-Lücken nicht aus. Andererseits braucht ein Unternehmen auch nicht zwangsläufig alle am Markt vorhandenen Sicherheitstechnologien einzusetzen, sondern kann diese von einem seriösen Provider modular ganz nach Bedarf beziehen. Spätere regelmäßige Risikobewertungen und Audits, etwa in Form von Penetrationstests, ergänzen diese ganzheitliche Sichtweise. So lassen sich neue Schwachstellen herausfinden und Maßnahmen schnell anpassen. Die genaue Auswahl und kontinuierliche Aktualisierung der Sicherheitsmaßnahmen ist gerade beim Cloud Computing sehr wichtig, da mit der hochgradigen Dezentralisierung und Verteilung von Anwendungen und Daten auch die Zahl der Angriffsvektoren und Gefahren steigt.

Sind die Sicherheitsanforderungen exakt festgelegt, lassen sie sich über Service Level Agreements durchgängig vertraglich vereinbaren, also von der Produktion im Rechenzentrum über die Netze bis zum PC oder mobilen Endgerät beim Anwender im Unternehmen. Im eigenen Netz kann der Dienstleister das Einhalten der **SLAs**¹² auch in der Cloud gewährleisten. So kann der Kunde die Qualität und die Verlässlichkeit des ICT-Service objektiv beurteilen.

Die Tatsache, dass eine spezialisierte, zentrale Stelle alle Vorgänge - Implementierung, Konfiguration, Release-, Update- und Patchmanagement, Backup etc. - kontrolliert und steuert, erleichtert das Einhalten der Sicherheitsmaßnahmen außerdem. Erst dadurch können diese auf sämtlichen Ebenen wie Zahnräder wirksam ineinander greifen. Das ermöglicht letztlich sogar das sichere Einbinden mobiler Endgeräte in die Wolke.

» 3. Anwendungen und Daten trennen

Trotz vieler Gemeinsamkeiten bei der Sicherheit stellt die virtuelle Wolke gegenüber dem klassischen Outsourcing einige besondere Anforderungen. Das betrifft zum Beispiel den Datenschutz: Da sich im Rechenzentrum mehrere Unternehmen Server teilen, die ihnen die jeweils benötigten Ressourcen zuweisen, muss sicher sein, dass niemand in die Daten des anderen einblicken kann. Hierzu kommt es auf eine saubere Trennung von Anwendungen und Daten der einzelnen Kunden an. Möglich machen das sogenannte virtuelle lokale Netzwerke (VLANs). Dabei erhält jeder neue Cloud-Kunde automatisch einen separaten Anschluss an den Server. Der Rechner verfügt somit am Ende über beliebig viele individuelle Zugangswege.

Die Administration von VLANs erfolgt mit einer zentralen Weiche (Switch). Hier laufen alle Netzwerkkabel zusammen. Der Switch ordnet jedes VLAN automatisch einem bestimmten Kunden zu. Dieser darf nur in seinem eigenen Bereich arbeiten. Die VLANs sind komplett voneinander isoliert. Jemand mit bösen Absichten käme so über den Switch gar nicht auf einen anderen Zugang.

Die Rechner selbst sollten in mehrere Einheiten partitioniert sein, von denen jeder Kunde eine Scheibe mitsamt VLAN-Zugang bekommt. Sie können somit nicht von ihrer Partition auf die eines anderen Unternehmens springen. Dadurch können zum Beispiel SAP- und Oracle-Anwendungen gemeinsam auf

einem Server laufen - strikt voneinander getrennt. Zudem sollten die Rechner vom öffentlichen Internet komplett entkoppelt sein. Webanwendungen, zum Beispiel für Online-Rechnungen, laufen dann in gesonderten Servicebereichen. Das unterbindet Angriffe übers Web auf geschäftskritische Anwendungen.

Letztlich sind die Informationen auch auf der Storage-Ebene voneinander zu isolieren. Sie lassen sich außerdem von der Technologie unveränderbar ablegen und sind damit revisions sicher archiviert.

» 4. Cloud-Systeme sicher integrieren

Einzelanwendungen liegen im Idealfall also im **Data Center**¹³ für jeden Kunden sicher voneinander isoliert vor. Gerade für Unternehmen kommt es aber oft darauf an, dass Applikationen miteinander kommunizieren. Die Mitarbeiter sollen beispielsweise E-Mails direkt aus SAP bearbeiten. Der **Cloud-Provider**¹⁴ kann hierzu getrennte Anwendungen eines Kunden in der Wolke wieder so zusammenführen, dass sie nach vorgegebenen Regeln gemeinsam funktionieren. Ein anderes Unternehmen bekommt hiervon nichts mit. Genauso ist auch eine Integration in die bestehende, nicht dynamische Anwendungslandschaft eines Kunden möglich, ohne dass für Angreifer Tür und Tor weit offenstehen. Selbst individuelle Einzelsysteme lassen sich einbinden, damit etwa unterschiedliche Fachabteilungen reibungslos miteinander arbeiten können.

Doch nicht nur andere Unternehmen sollten keinen Einblick in vertrauliche Informationen erhalten. So sollte ein **Cloud**¹⁵-Nutzer auch seinen Provider fragen, wie er es selbst mit Zugriffsrechten hält. Besonders kritische Daten sollten im **Rechenzentrum**¹⁶ so abgelegt sein, dass auch Mitarbeiter des Dienstleisters sie nicht einsehen, verändern oder löschen können. Lässt es sich für eine bestimmte Operation nicht vermeiden, auf die Informationen zuzugreifen, muss der Dienstleister seinen Kunden vorher um Erlaubnis fragen. Nur er besitzt den Schlüssel zu den Daten.

Sollte der Kunde irgendwann aus der Wolke aussteigen wollen, müssen die Informationen lückenlos an ihn zurückfließen. Aus diesem Grund sollten Unternehmen vor der Auftragsvergabe auch auf die wirtschaftliche Stabilität des Dienstleisters achten. Unter Umständen leidet unter einer Insolvenz die Verfügbarkeit der Daten.

» 5. Identitäten prüfen und managen

Aber auch beim Kunden dürfen nach dem "Need-to-know"-Prinzip nur berechnigte Mitarbeiter die Informationen einsehen, die sie für ihre Arbeit tatsächlich brauchen. Aus dem klassischen Outsourcing bekannte Verschlüsselungs- und Zugangsmechanismen unterstützen solch ein Rollen- und Rechtemanagement. Public-Key-Infrastrukturen (PKI) stellen zum Beispiel sicher, dass sich der richtige Mitarbeiter am System anmeldet. Sie schalten den Zugang erst nach erfolgreicher Identifikation frei, zum Beispiel über Chipkarten mit Signaturfunktion, biometrische Verfahren oder über die mit einem Einmalpasswort versehene SIM-Karte (Subscriber Identity Module) im Handy. Damit verhindert eine PKI das Mitlesen oder Umlenken von Kommunikationsbeziehungen beziehungsweise das Einspielen von Schadsoftware ins Netz.

Große **Cloud**¹⁷-Provider besitzen eigene Trust Center, die Zertifikate zur Authentisierung an einem System herausgeben. Erst mit diesen digitalen Ausweisen erhält der berechnigte Nutzer Zugang. Auf der anderen Seite können sich Mitarbeiter mit den ihnen zugeteilten Zertifikaten auch gegenseitig zuverlässig erkennen. Nach dem Austausch der Ausweise weiß jeder, dass auf der anderen Seite tatsächlich der erwartete Ansprechpartner mit ihm kommuniziert. So lassen sich auch in Cloud-Beziehungen sichere abteilungs- und unternehmensübergreifende Netzwerke für die Zusammenarbeit einrichten.

» 6. Wo liegen die Daten?

Zu großer Unsicherheit im Cloud Computing führt auch ein Faktor, der sich vom klassischen Outsourcing grundsätzlich unterscheidet: Der Nutzer weiß im Normalfall nicht, auf welchen Systemen, in welchem Rechenzentrum und - vor allem - in welchem Land der Provider seine Daten speichert. Diese Katze im Sack kann sich fürs Geschäft fatal auswirken. Überschreiten die Daten Ländergrenzen, erfüllen sie möglicherweise wichtige Anforderungen an die Sicherheit oder rechtliche und branchenspezifische Auflagen nicht. So ist es in Frankreich und Polen nicht erlaubt, Finanzdaten außerhalb des Landes zu betreiben. In den USA und anderen Ländern fallen Sicherheitstechnologien wie Verschlüsselung unter das Kriegswaffenkontrollgesetz und sind daher nur in Ausnahmefällen zulässig. Häufig ist auch nicht geregelt, wer im Fall eines Datenverlusts im Staat XY die Haftung trägt und wie diese aussieht.

Weiterhin bestehen Risiken durch unterschiedlich gestaltete Gesetzgebungen, zum Beispiel beim Abhören oder bei unbemerkten Zugriffen. In einigen Staaten können Behörden jederzeit ohne Vorwarnung die

Herausgabe vollständiger Backups verlangen. Die Liste der Unterschiede in Bezug auf den Datenschutz lässt sich nahezu unendlich weiterführen. Manch ein internationaler ICT-Dienstleister verzichtet deshalb bewusst darauf, in bestimmten Ländern ein eigenes Rechenzentrum zu errichten. In der Private Cloud von T-Systems kann der Nutzer darüber hinaus selbst bestimmen, wo er seine Daten abgelegt haben möchte.

» 7. EU-Datenschutz erleichtert Cloud-Nutzung

Für [Cloud-Services](#)¹⁸ im geschäftlichen Umfeld eignen sich besonders Anbieter aus der Europäischen Union. Mit der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr hat die EU einen Mindeststandard für den [Datenschutz](#)¹⁹ und die Datensicherheit eingeführt. So setzt zum Beispiel jede Übermittlung personenbezogener Informationen die vorherige Einwilligung des Betroffenen voraus. Auftragsdaten dürfen nur in den Grenzen der EU beziehungsweise des Europäischen Wirtschaftsraums (EWR) verarbeitet werden. Öffentliche Institutionen verknüpfen Vergaben oft mit einer Datenverarbeitung im eigenen Land. Erstaunlicherweise gibt es selbst in den USA bislang keine festgeschriebenen Richtlinien zum Datenschutz. Dort sind nur spezielle Arten der Verarbeitung verboten. Behördenakten beispielsweise sind von jedem Bürger problemlos abrufbar.

Das Wissen, wo die Daten liegen, hat darüber hinaus noch einen anderen Aspekt: Manche Großunternehmen wollen ihre Daten und Anwendungen in einem ausfallsicheren Rechenzentrum wissen, das auch von der geographischen Lage her vor Naturkatastrophen - Erdbeben, Stürme, Überschwemmungen etc. - gut geschützt sind. Ein internationaler Mineralölkonzern bezieht deshalb bereits bewusst Cloud-Computing-Services aus München.

» 8. Datentransport absichern

Das Rückgrat jeder [Cloud](#)²⁰ bilden stabile, breitbandige Netze. Die Informationssicherheit lässt sich hier auf zwei Wegen gewährleisten. Den höchsten Schutz bieten dedizierte Punkt-zu-Punkt-Verbindungen, vom Rechenzentrum zum Kunden. In MPLS-Netzen lässt sich für jeden Kunden eine vollständig isolierte Leitung einrichten. Die zweite Möglichkeit sind verschlüsselte Verbindungen, entweder über getunnelte Verbindungen im öffentlichen Internet (VPN, Virtual Private Networks) oder über SSL (Secure Socket Layer).

Aber wie auch immer die Netzverbindung konkret realisiert wird, sie sollte genau wie beim normalen Outsourcing doppelt ausgelegt sein und über zwei voneinander getrennte physikalische Verbindungen laufen. Fällt dann eine der beiden Leitungen aus, kann die andere nahtlos den Dienst der anderen übernehmen. Zudem empfiehlt es sich, alle Informationen gespiegelt in zwei verschiedenen Rechenzentren vorzuhalten. Das ist kein Widerspruch zur Cloud, wenn an beiden Standorten die Möglichkeit besteht, Server zwischen mehreren Unternehmen aufzuteilen.

» 9. Brandmauern schützen Netzsegmente

Zum Schutz der verschiedenen Netzsegmente dienen [Firewalls](#)²¹. Sie kontrollieren den Datenverkehr und bestimmen regelbasiert, welche Pakete sie durchs Netzwerk schleusen und welche nicht. Das bietet Schutz vor unerlaubten Zugriffen. Zusätzlich erstellen sie Status- und Kontexttabellen aller Netzwerkverbindungen und erkennen so Korrelationen zwischen den Paketen (Stateful Inspection). Dadurch erkennen sie nach einem Verbindungsaufbau, ob ein System unaufgefordert Daten sendet und blockieren diese. Viele Pakete gleichen Typs weisen etwa auf eine Denial-of-Service-(DoS)-Attacke hin, die das Netzwerk lahmlegen soll. Firewalls sind damit auch ein wichtiger Erkennungsmechanismus, um die Verfügbarkeit von Daten und Anwendungen sicherzustellen. Sogenannte Computer Emergency Response Teams (CERT) achten im Rechenzentrum unter anderem darauf, dass sie jederzeit korrekt konfiguriert sind.

Einen Schritt weiter gehen Deep Inspection Firewalls, die Angriffe auf der Anwendungsebene erkennen. Sie blockieren Protokollverletzungen, Viren, Spam und weitere schädliche Inhalte wie etwa Trojaner. Das erschwert auch sogenannte Man-in-the-Middle-Attacken, bei denen Dritte die Kommunikation zwischen zwei Kommunikationspartnern abfangen und eine von beiden Parteien zu ungewollten Aktionen verleiten, indem sie sich als der vermeintliche Partner ausgeben. Mitarbeiter von Cloud Providern führen solche Angriffe in regelmäßigen Abständen durch, um die Wirksamkeit der Firewall zu testen.

» 10. Monitoring und Frühwarnsysteme nutzen

Damit Sicherheit zu einem integralen Bestandteil aller Geschäftsprozesse im Cloud Computing wird, müssen sie kontinuierlich auf sicherheitsrelevante Komponenten überprüft und aktualisiert werden. In großen Rechenzentren sorgen spezielle Module auf den Servern automatisiert dafür, dass die vorgegebenen Sicherheitseinstellungen sich nicht verändern. Auch alle Firewalls, Virens Scanner und Intrusion Detection

Systeme (IDS) befinden sich unter ständiger automatischer Überwachung. Frühwarnsysteme spüren auf der Basis von Data-Mining-Verfahren Schwachstellen auf, bevor sie sich gefährlich auswirken. Angreifer nehmen sich oftmals viel Zeit, um über mehrere Stationen eine Lücke zu finden und einzudringen. Intelligente Analysensysteme (Security Information und Event Management) erkennen hierzu unter anderem anhand von Logfiles auffällige Muster und unterbinden solche Langzeitangriffe rechtzeitig.

Auch nach bestimmten Regularien lässt sich die IT-Infrastruktur im Rechenzentrum automatisiert überwachen, beispielsweise nach dem [Sarbanes-Oxley²²](#) Act (SOX). Dieses Kapitalmarktgesetz ist für an US-amerikanischen Börsen notierte Unternehmen relevant. Sie müssen ihr Internes Kontrollsystem (IKS) jährlich anhand seiner Richtlinien überprüfen, dokumentieren und von Wirtschaftsprüfern testieren lassen. Die Passwörter des Systems müssen alle eine bestimmte Länge aufweisen. Ist das nicht der Fall, merkt das eine Lösung im Rechenzentrum und Mitarbeiter des präventiven CERT-Teams können sofort nachsteuern.

» 11. Security beginnt in den Köpfen

Trotz aller Sicherheit, die ein großer [Cloud²³](#)-Provider bieten kann: Am Ende beginnt [Security²⁴](#) in den Köpfen der Mitarbeiter. Regelmäßige Workshops und Schulungen können die generelle Wachsamkeit im Umgang mit ICT-Lösungen steigern. Nur wer mögliche Sicherheitsprobleme kennt, kann sie durch richtiges Verhalten umgehen. Einige Dienstleister veranstalten interne und externe Programme, um das allgemeine Schutzniveau zu steigern und die richtige Sicherheitspolitik für ein Unternehmen zu entwickeln. Dass die Systeme anschließend alle so gestaltet sind, dass die Nutzer sie trotz aller Sicherheitsfunktionen noch sinnvoll einsetzen können, ist die Kunst des Cloud-Providers.

» 12. Mobile Cloud-Zugänge absichern

Bezieht ein Unternehmen alle Dienste und Daten über ein IP-Netz aus einem [Cloud²⁵](#)-Rechenzentrum, können Mitarbeiter mit einem beliebigen Endgerät überall und jederzeit sicher auf ihre persönliche Nutzeroberfläche zugreifen. Sie melden sich hierzu mittels einem [USB²⁶](#)-Stick mit integrierter Smartcard am zentralen Server im Rechenzentrum an und können das Endgerät genauso nutzen wie einen klassischen Laptop - im Hotel, am Flughafen, beim Geschäftspartner oder im Internetcafe. Stecken die Anwender den Stick in den USB-Anschluss des mit dem Internet verbundenen Rechners, stellt er über den integrierten Client automatisch eine verschlüsselte Verbindung zu einer Gegenstelle im Rechenzentrum her. Nach erfolgreicher Authentifikation erhält der Nutzer dann den Zugriff auf seine Daten und Applikationen. Zieht er den Stick wieder aus dem Desktop heraus, verbleiben auf dem Rechner keine Datenspuren.

Handys, PDAs und Smartphones, auf denen Applikationen installiert sind, lassen sich genauso zuverlässig verschlüsseln. Auch hier muss sich der Nutzer über eine Kryptokarte zunächst identifizieren. Kommt ihm das Endgerät abhanden, lässt es sich von Mitarbeitern im Rechenzentrum aus der Ferne in seinen Auslieferungszustand zurückversetzen. So gelangen Daten nicht in fremde Hände. Gleichzeitig gehen dem Unternehmen keine wertvollen Informationen verloren, da diese vollständig im Rechenzentrum gespeichert vorliegen. Während des normalen Betriebs findet automatisch eine regelmäßige Synchronisation aller Daten auf dem Endgerät mit den zentralen Servern statt.

Sicherheitsrichtlinien eines Unternehmens sind somit in der Wolke auch mobil umsetzbar: So lassen sich bestimmte Funktionen von Endgeräten in bestimmten Bereichen automatisiert abschalten, beispielsweise integrierte Kameras. Auf diese Weise gelangen in der Fertigungsindustrie keine Bilder von neuen Produkten ungewollt in fremde Hände oder ins Internet.

Auch das Qualitätsmanagement erleidet keine Einbußen: Die Security-Experten im Rechenzentrum können neuen Patches in Ruhe prüfen, bevor sie sie auf die Rechner aufspielen. Ist für eine Sicherheitslücke, die eine akute Bedrohung für Laptops & Co bedeutet, noch kein elektronischer Flicker vorhanden ("Day-Zero-Problem"), können sie die entsprechenden Zugänge kurzfristig per Knopfdruck aus der Ferne blockieren. (wh)

¹ <http://www.computerwoche.de/management/cloud-computing/>

² <http://www.computerwoche.de/security/>

³ <http://www.computerwoche.de/management/cloud-computing/1881599/>

⁴ <http://www.computerwoche.de/schwerpunkt/c/Cloud-Computing.html>

⁵ <http://www.computerwoche.de/schwerpunkt/a/amazon.html>

⁶ <http://www.computerwoche.de/schwerpunkt/g/google%20cloud.html>

⁷ <http://www.computerwoche.de/security/>

⁸ <http://www.computerwoche.de/management/cloud-computing/1881599/>

⁹ <http://www.computerwoche.de/security/>

¹⁰ <http://www.computerwoche.de/security/>

- 11 <http://www.computerwoche.de/security/>
- 12 <http://www.computerwoche.de/schwerpunkt/s/SLAs.html>
- 13 <http://www.computerwoche.de/hardware/data-center-server/2016541/>
- 14 <http://www.computerwoche.de/management/cloud-computing/1881599/>
- 15 <http://www.computerwoche.de/management/cloud-computing/1881599/>
- 16 <http://www.computerwoche.de/hardware/data-center-server/2016541/>
- 17 <http://www.computerwoche.de/management/cloud-computing/1881599/>
- 18 <http://www.computerwoche.de/management/cloud-computing/1881599/>
- 19 <http://www.computerwoche.de/schwerpunkt/d/datenschutz.html>
- 20 <http://www.computerwoche.de/management/cloud-computing/1881599/>
- 21 <http://www.computerwoche.de/schwerpunkt/f/firewall.html>
- 22 <http://www.computerwoche.de/schwerpunkt/s/Sarbanes-Oxley.html>
- 23 <http://www.computerwoche.de/management/cloud-computing/1881599/>
- 24 <http://www.computerwoche.de/security/>
- 25 <http://www.computerwoche.de/management/cloud-computing/1881599/>
- 26 <http://www.computerwoche.de/schwerpunkt/u/usb.html>

IDG Business Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Media GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in Computerwoche unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von Computerwoche aus gelinkt wird, übernimmt die IDG Business Media GmbH keine Verantwortung.