IT-Compliance &
IT-Governance

Produkte &
Technologien

Security &
Cloud Computing

Microsoft

Kompendium
IT-Compliance und -Security

Für jede Anforderung der passende Cloud-Service
„Cloud OS" von Microsoft – so finden Sie die beste Kombination verschiedener Cloud-Services und das optimale Betriebsmodell

Schritt für Schritt zum IT-Compliance-Management
Mit einer systematischen und schrittweisen Vorgehensweise zu dauerhafter Rechtssicherheit und Richtlinienkonformität

Notfall-Management als Management-Aufgabe
So führen Sie Ihr operatives Geschäft auch bei einem Schadensereignis kontrolliert und strukturiert fort

Immer im Lieblingsbüro

Office 365 ermöglicht die Zusammenarbeit von praktisch überall aus. Dank zentraler Speicherung und gesicherter Dokumentenfreigabe steht Ihren Mitarbeitern immer der aktuellste Stand der Dateien zur Verfügung – und das geräteunabhängig. Durch das flexible Arbeiten steigt nicht nur die Produktivität, sondern auch die Zufriedenheit. Entdecken Sie, wie Sie clever die Möglichkeiten von Office 365 für sich und Ihr Unternehmen nutzen können. Original Office auf bis zu 5 Endgeräten zur Miete. Mehr erfahren auf office.com/business

Office 365

Inhalt

griffity®
www.griffity.de

Wir bringen Kompetenz & Pepp in Ihre Projekte!

COLOR YOUR MARKETING

Spannende, erfolgreiche Werbung für faszinierende Technik – griffity hat die Farben, die ins Schwarze treffen. Das ist entscheidend, denn den richtigen Ton zu finden zwischen schrill und mausgrau, ist nicht immer ganz einfach – aber genau darauf kommt es an. Gerade im B2B-Bereich ist seriöses Auftreten gefragt – trotzdem bedarf es farblicher Akzente. Und um rundum positiv hervorzustechen, statt unangenehm ins Auge zu fallen, geht es vor allem um die richtige Farbgestaltung.

Haben wir Sie neugierig gemacht? Dann stellen Sie unsere Kreativität und Professionalität am besten auf die Probe!

Unser Full-Service-Spektrum:

Design: Das professionelle Outfit für Ihr Unternehmen • Text: Treffsicher und nutzenorientiert • Produktion: Qualität ohne Wenn und Aber Media: Planung und Steuerung durch Profis • Werbegeschenke • Event-Marketing • Direct-Marketing • Interactive & Bewegte Bilder Video Synchros & 3D-Animationen • Web & HTML • Social Media • Public Relations: Pressemitteilungen, Fachartikel & Case Studies

griffity GmbH · Hanns-Schwindt-Straße 8 · 81829 München Deutschland · Telefon +49 (0)89 - 43 66 92-0 · Fax +49 (0)89 - 43 66 92-66
info@griffity.de · www.griffity.de

Editorial

Michael Kranawetter,
Chief Security Advisor
Microsoft Deutschland GmbH

Sehr geehrte Leserinnen und Leser,

Computerbetrug, Datenmanipulation, Datendiebstahl, Betrug mit Zugangsberechtigungen und Sabotage – die Zahl der Bedrohungen im Bereich der Cyberkriminalität steigt jedes Jahr erheblich. Die Schätzungen über die Schäden liegen dabei in dreistelligen Millionenbeträgen bis hin zu Schäden in Milliardenhöhe. Dabei sind die Einbußen, die Unternehmen durch Malware und andere Bedrohungen entstehen, noch gar nicht eingerechnet.

Verfolgen Sie einen ganzheitlichen Ansatz. Wir empfehlen Unternehmen, eine umfassende und durchgängige Sicherheitsinfrastruktur aufzusetzen, die neben Lösungen für die physische Absicherung, die Netzwerk-, System- und Anwendungssicherheit auch Richtlinien, Guidelines, Prozesse und Dokumentationen umfasst. Dabei ist es ebenso wichtig, das Sicherheitsniveau im Unternehmen regelmäßig zu prüfen, zu bewerten und Audits durchzuführen – möglicherweise auch zusammen mit einem externen Partner und Sicherheitsexperten. Nicht zuletzt gilt es, die Mitarbeiter im Unternehmen für das Thema Sicherheit zu sensibilisieren und zu informieren, damit sie – trotz einer sicheren technischen Infrastruktur – die notwendige Vorsicht walten lassen.

Bleiben Sie auf dem Laufenden. Mit dieser Ausgabe des Microsoft Kompendiums „IT-Compliance und -Security" möchten wir Sie dabei unterstützen, die für Ihr Unternehmen passende Sicherheitsinfrastruktur aufzusetzen und die richtigen Lösungen zu finden. Sie finden Hilfestellungen für den Aufbau einer Sicherheitsinfrastruktur, Hintergrundwissen zu aktuellen Themen und innovativen Produkten und Technologien sowie Handlungsempfehlungen und Informationen rund um die Themen IT-Compliance & IT-Governance.

Wir wünschen Ihnen viel Freude beim Lesen!

Herzlichst Ihr

Michael Kranawetter
Chief Security Advisor
Microsoft Deutschland GmbH

Herausgeber:
griffity
Griffity GmbH
Hanns-Schwindt-Str. 8, 81829 München
Telefon 089 43 66 92 0
www.griffity.de

Mit freundlicher Unterstützung
von Microsoft

Redaktion:
Michael Kranawetter
Chief Security Advisor
Microsoft Deutschland GmbH

Grafik, Layout und Produktion:
Griffity GmbH, München
www.griffity.de

„Cloud OS“ von Microsoft als übergreifende Lösung für moderne Unternehmen

Für jede Anforderung der passende Cloud-Service

Microsofts Cloud-Strategie ermöglicht es, Dienste und Anwendungen in bestehenden On-premise-Installationen (Private Cloud) mit Diensten in der Service-Provider-Cloud (Hosted Private Cloud) oder der Microsoft Public Cloud nahtlos zu verbinden. Dank einheitlicher und übergreifender Technologien können Unternehmen das optimale Betriebsmodell und die beste Kombination verschiedener Cloud-Services – unabhängig von technologischen Abhängigkeiten – für sich wählen.

Der IT-Markt ist heute von zahlreichen Veränderungen geprägt. Drei wichtige Trends, die direkten Einfluss auf die Entscheidungen der Unternehmen haben, sind Cloud-Lösungen, die zunehmende Abhängigkeit der Unternehmen von der eingesetzten IT und die steigende Sensibilität beim Umgang mit Daten und Datenschutz. Die Bedeutung cloudbasierender IT-Lösungen zeigt sich sehr deutlich an den Wachstumszahlen. So wächst der deutsche IT-Markt 2013 gegenüber dem Vorjahr laut Bitkom um 2,2 Prozent, während das Marktforschungsunternehmen Experton für Cloud-Services (IaaS, PaaS, SaaS) im Jahr 2013 ein Wachstum von 63 Prozent prognostiziert. Die zunehmende Abhängigkeit der Unternehmen von der eingesetzten IT resultiert aus der steigenden Integration IT-gestützter Prozesse in die Wertschöpfungsketten und aus der veränderten Arbeitsweise sowie der Verarbeitung von Informationen. Beispielhafte Trends sind die Industrie 4.0, das „Mobile Unternehmen der Zukunft“ (IDC) oder „The Internet of Things“. Im gleichen Maß wie das Angebot an cloudbasierenden Lösungen und die Verzahnung der IT mit allen Geschäftsfeldern steigt, steigt auch der Bedarf an Information und Kontrolle. Daten werden nicht mehr nur im Unternehmen gespeichert und verarbeitet, sondern auch Lieferanten und Partnern auftragsbezogen zur Verfügung gestellt. Spätestens, wenn es sich hierbei um personenbezogene Daten handelt, muss der ordnungsgemäße Umgang mit den Informationen sichergestellt und nachweisbar sein.

Hohe Datenschutz-Standards als Chance

In Europa und insbesondere in Deutschland existieren besonders strikte Regeln für den Umgang mit und die Speicherung von Daten, die es nicht ohne Weiteres zulassen,

beliebige IT-Systeme in eine Cloud zu überführen. Auf EU-Ebene ist die Richtlinie 95/46/EG maßgeblich, die den Mindeststandard für Datenschutz aller Mitgliedsstaaten definiert. Auf lokaler Ebene ist vor allem das Bundesdatenschutzgesetz (BDSG) zu beachten. Es wird durch die Datenschutzgesetze der Länder und bereichsspezifischen Regelungen ergänzt. Für IT-Service-Provider bedeutet dies, dass sie entsprechende Prozesse etablieren müssen, um nachweisen zu können, dass ihr IT-Betrieb den verschiedenen, teilweise kundenindividuellen Anforderungen gerecht wird. Gleichzeitig profitieren lokale Service-Provider von den hohen lokalen Anforderungen an Datenschutz und Datensicherheit, die den Einsatz globaler Cloud-Dienste erschweren.

Die Rolle des CIOs im Wandel

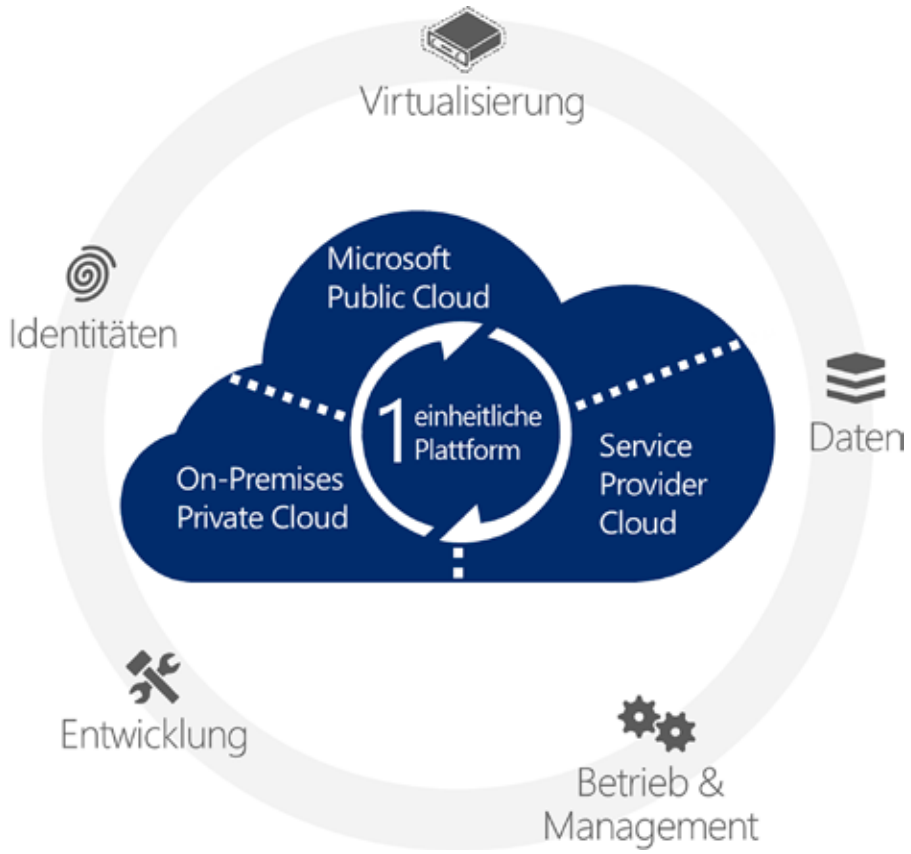
Für Unternehmen, die über die Auslagerung ihrer IT oder auch nur bestimmter Komponenten ihrer IT-Infrastruktur nachdenken, bedarf es einer genauen Prüfung, welcher Kritikalität und welchen datenschutzrechtlichen Anforderungen die entsprechenden IT-Systeme unterliegen. Dies geht einher mit dem grundlegenden Wandel der CIO-Rolle im Unternehmen, wie sie beispielsweise Experton und Forrester beschreiben. Die Rolle des CIOs wird künftig in ihrer Relevanz steigen. Im Rahmen von Sourcing-Entscheidungen umfasst dies auch eine engere Zusammenarbeit mit den Fachabteilungen und eine umfassende Auseinandersetzung mit dem Thema Datenschutz. Unkritische Geschäftsprozesse können in eine Public Cloud ausgelagert werden. Unternehmen profitieren hierbei von hoher Flexibilität und dem größten Kosteneinsparpotenzial. Geschäftsprozesse mit hoher Kritikalität und hohen Datenschutzanforderungen können im eigenen Rechenzentrum verbleiben oder mit definierten Compliance- und Datenschutz-Vorgaben an einen Service-Provider übergeben werden.

Die Zukunft ist hybrid

Gemäß einer Analyse von Microsoft glauben 100 Prozent der CIOs von Großunternehmen, die sich mit Cloud-Technologien auseinandersetzen, an eine „hybride Zukunft" – also die Kombination verschiedener Betriebsmodelle –, um ihren IT-Bedarf optimal abdecken zu können. Dies bedarf einheitlicher, übergreifender Technologien, um verschiedene Geschäftsprozesse, Applikationen und Daten, die in unterschiedlichen Betriebsmodellen implementiert sind, übergreifend steuern und kontrollieren zu können.

Verschiedene Betriebsmodelle nahtlos verbinden

Mit der Strategie „Cloud OS" bietet Microsoft als einziger Hersteller eine einheitliche und übergreifende Technologie-Plattform, die die verschiedenen Betriebsmodelle nahtlos miteinander verbindet. Die Strategie „Cloud OS" basiert technologisch auf den etablierten On-premise-Produkten – ergänzt um die Erfahrungen aus dem eigenen Betrieb hochskalierender und verteilter Cloud-Lösungen. Das Design-Prinzip aller Komponenten lautet „Cloud first": Anstatt nachträglich Dienste „cloud-ready" zu machen, wird von Anfang an auf Interopera-

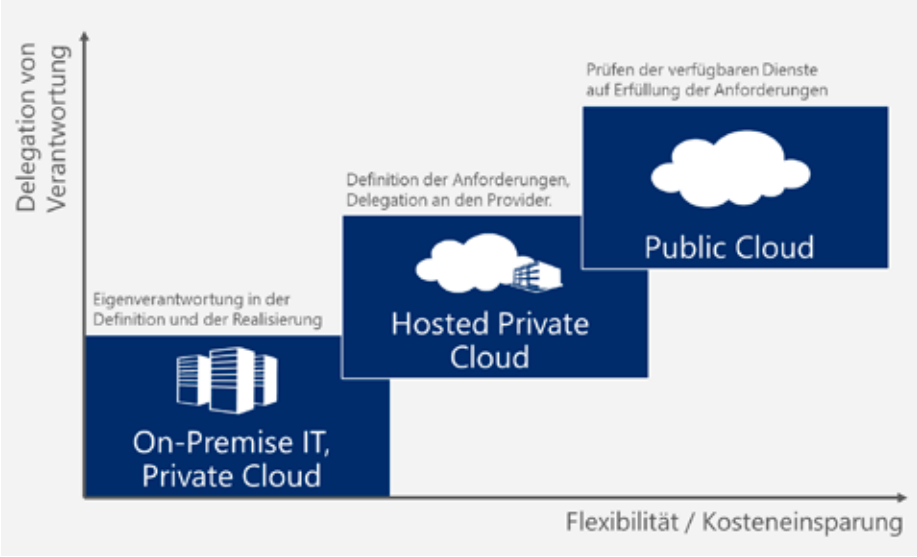


Microsofts Cloud-Strategie „Cloud OS"

bilität und Kompatibilität geachtet. So sind die Erfahrungen aus dem jahrelangen Betrieb weltweiter Plattformen wie Outlook.com, Dynamics CRM Online, Xbox Live oder Bing in die Weiterentwicklung der Server-Produkte wie Windows Server 2012 R2 und System Center 2012 R2 eingeflossen. Für Service-Provider wird es damit einfacher, hocheffiziente und sichere (Hosted) Cloud-Infrastrukturen für ihre Kunden aufzubauen und anzubieten. Gleichzeitig können auch Service-Provider ihre IT-Services um Komponenten der Public Cloud ergänzen, wie beispielsweise den Azure Global Service Monitor. Die Daten des Kunden verbleiben im zertifizierten und nach deutschem Recht gesicherten Rechenzentrum. Der Service Provider kann weltweite Service-Levels überwachen – ohne auf verschiedenen Kontinenten eigene Messsysteme zu betreiben. Für Kunden, die ihre IT bisher vollständig im eigenen Rechenzentrum betrieben haben, ergeben sich neue Möglichkeiten, Komponenten ihrer IT-Infrastruktur in eine Hosted Private Cloud oder eine Public Cloud auszulagern. Sollen die Verwaltung und die Administration der Anwendung in eigener Hand bleiben, bietet sich IaaS (Infrastructure as a Service) oder PaaS (Platform as a Service) bei einem Service-Provider oder mit Windows Azure an. Die zusätzlichen Cloud-Ressourcen lassen sich im System Center des Kunden dank einheitlicher Technologien einbinden und verwalten. Soll auch die Administration der Anwendung ausgelagert werden, können Unternehmen SaaS (Software as a Service) in einer Public Cloud oder die individuellen Lösungen eines Service-Providers nutzen.

Die optimale Cloud-Strategie umsetzen

Laut einer IDC-Studie im Auftrag von Microsoft erwarten 74 Prozent der Befragten von ihrem Cloud-Anbieter, dass er in der Lage ist, einen Dienst auch wieder in die On-premise-Infrastruktur zu transferieren. 84 Prozent der Befragten sehen eine bewährte Partnerschaft als Voraussetzung, um einem Cloud-Anbieter zu vertrauen. Microsoft ermöglicht dies mit der Strategie „Cloud OS" sowie dem Angebot aus Partner-Hosting und den Diensten der Microsoft Public Cloud. Ausgehend von den individuellen Anforderungen und Bedarfen eines Unternehmens wird es mit Hilfe von Microsofts Cloud-Technologie möglich, die optimale Cloud-Strategie zu finden und umzusetzen. Microsoft und die Partner des Unternehmens unterstützen Sie dabei. ■



Unterschiedliche Betriebsmodelle moderner IT

Karsten Hartlieb ist als Produkt Marketing Manager innerhalb der Server Tools und Cloud Business Group tätig. Sein besonderes Augenmerk gilt dabei den verschiedenen Hosting-Partnern und der Vermarktung von Microsofts Server-Produkten für den erfolgreichen Einsatz im Hosting-Betrieb oder in Managed-IT-Umgebungen.

Supporting your business. Anytime, anywhere.

unique projects

Effektive IT & Virtualisierung haben einen Namen: unique projects.

Microsoft Partner
Silver Midmarket Solution Provider
Silver Hosting
Silver OEM

Wir sind angetrieben von der weltweiten Vernetzung der Geschäftsprozesse. Remote-Zugriffe und individuelle Services rufen nach Virtualisierung auf allen Ebenen. Desktops sind überall und jederzeit nutzbar. Ebenso lassen sich immer mehr Anwendungen und Serverlandschaften zentral im Rechenzentrum virtualisieren. Der User wird noch mobiler und unabhängiger. Wir verwalten Ihre Arbeitsplätze übersichtlich, bequem und rund um die Uhr, im zentralen Rechenzentrum.

Ihre IT hat noch viel Konsolidierungspotential und „Luft nach unten“

Noch schlanker, effizienter und günstiger. So könnte Ihre IT bald aussehen. Die konsequente Virtualisierung von Servern verheißt einen geringeren Bedarf an Hardware, eine bessere Auslastung und flexiblere Nutzung vorhandener Ressourcen, ein einfacheres Server-Management, eine höhere Ausfallsicherheit sowie eine nachhaltige Senkung der Betriebskosten für Administration, Stromversorgung und Klimatisierung.

„Die Beziehung zwischen uns und unseren Kunden ist fast wie bei einem Ehepaar.“ ...

Sven Pöhlsen, Geschäftsführer

Kundenorientierung, Transparenz und Klarheit über die Ziele sind die Grundlagen unserer Leistungen.

Und unsere Erfahrung, unser Fachwissen und die Vielfalt unserer Angebote sind die Instrumente, mit denen wir am Markt brillieren. Weil sie uns gemeinsam schnell, sicher und professionell dokumentiert ans Ziel bringen. Applaus? Bekommen wir für unsere Erfahrung und unser umfassendes Produkt-Know-how, die die Realisierung von Projekten erleichtern. Und da capo? Können wir sagen, wenn es um die fortlaufende Weiterbildung und -entwicklung unserer Spezialisten geht: Sie beschäftigen sich intensiv mit den neuen Technologien, die wir Ihnen anbieten. Sie können sich sehr schnell in vorhandene IT-Umgebungen einarbeiten und auf neue oder zusätzliche Anforderungen reagieren. Und sie wissen ganz genau, wie Software und Hardware konfiguriert werden müssen, damit alle Systeme harmonieren. Beste Unterstützung also, auf die Sie sich zu jeder Zeit verlassen können.

... „Nur, dass bei uns zu 99 % Zufriedenheit herrscht.“

Sven Rodewald, Geschäftsführer

unique projects GmbH & Co. KG
Stresemannstraße 78–80
47051 Duisburg-Innenhafen

T: +49 203 709009-0
E: sales@unique-projects.com
W: www.unique-projects.com

Microsoft Partner · Dell PartnerDirect Preferred · VMware Partner Enterprise Solution Provider · Citrix Partner Silver Solution Advisor · Sophos

Microsoft

Mehr Sicherheit für Ihre Infrastruktur

Bedrohungen erkennen und Angriffe gezielt abwehren

Weltweit werden mehr und mehr Unternehmen das Angriffsziel von Cyberkriminellen. Dabei lassen sich bestimmte Angriffsformen wie Passwort-Diebstahl mit einem durchdachten Sicherheitskonzept und gezielten Maßnahmen sehr effektiv abwehren. Microsoft unterstützt Unternehmen mit zahlreichen Service-Angeboten und umfassenden Handlungsempfehlungen dabei, ihre IT-Infrastruktur wirkungsvoll abzusichern.

Seit Jahrzehnten werden die Microsoft Consulting Services (MCS) in großen und komplexen IT-Projekten bei Fragestellungen zur IT-Sicherheit hinzugezogen. In gleichem Maße wie die Technologie hat sich auch die Ausgangslage der Kunden signifikant verändert. Noch vor ein oder zwei Jahren gingen viele Unternehmen davon aus, dass ihr Netzwerk und ihre Infrastruktur als sicher zu betrachten seien, was sich auch im Design ihrer IT-Lösungen manifestierte. Dies ist sicher eine allzu optimistische Annahme gewesen. Heute ist diese positive Grundhaltung in den meisten Unternehmen einer gewissen Skepsis gewichen. Dass dies nicht unbegründet ist, sehen die Teams der Microsoft Cyber Security Group jeden Tag.

Hohe Expertise im Bereich Sicherheit

Weltweit nehmen die Anfragen rund um potenziell kompromittierte Unternehmensnetzwerke zu. Da auch Microsoft mit seinen zahlreichen Onlinediensten und seiner Präsenz auf dem weltweiten IT- und Services-Markt ein attraktives Ziel ist, ist die Domäne des Unternehmens eine der meist angegriffenen im Internet. Deshalb verfügen die Engineers, Berater und Architekten von Microsoft auch über eine hohe Expertise im Bereich Security und sind begehrte Gesprächspartner für die Sicherheitsbeauftragten, CIOs und CISOs von Unternehmen jeder Größe und jeder Branche.

Service-Angebote von Microsoft

Microsoft reagiert auf die steigende Nachfrage nach Unterstützung bei der Erkennung, Untersuchung und Bekämpfung von böswilligen Angriffen mit einem umfassenden Maßnahmenpaket. Das Unternehmen bietet neue Service-Angebote, um potenziell kompromittierten Unternehmen dabei zu helfen, die Angreifer aus dem Unternehmensnetzwerk zu entfernen. Darüber hinaus bietet Microsoft den Unternehmen umfassende Informationen sowie Empfehlungen zur Selbsthilfe. Das Microsoft Cyber Security Team hat die Erfahrung gemacht, dass Unternehmen, die diese Empfehlungen konsequent umsetzen, die Angriffsfläche drastisch reduzieren können.

Eine genaue Beschreibung der grundlegenden Prinzipien von „Pass the Hash" sowie der empfohlenen Maßnahmen gegen diese Angriffsmethode finden Sie unter:

Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques
http://www.Microsoft.com/en-us/download/details.aspx?id=36036

Securing Active Directory: An Overview of Best Practices
http://technet.Microsoft.com/en-us/library/dn205220.aspx

Microsoft Security Intelligence Report (SIR)
http://www.Microsoft.com/security/sir/default.aspx

Wichtige Handlungsempfehlungen

Häufig versuchen Angreifer, „von Rechner zu Rechner zu springen" (Lateral Movement) und die Berechtigungen derjenigen Benutzerkonten zu erweitern, die in der ersten Phase des Angriffs kompromittiert wurden (Privilege Elevation). Dieses Verfahren kommt vor allem dann zum Tragen, wenn ein Single-Sign-On (SSO) im Netzwerk möglich ist. Dieser Angriff heißt „Pass the Hash" (PtH). In der Abbildung 1 ist der erste Schritt eines PtH-Angriffs dargestellt. Beim einem „Pass the Hash"-Angriff werden die Hashes der Konten ausgelesen, die lokal im System angemeldet sind und deren Password-Hash in der lokalen Security-Account-Manager-Datenbank (SAM) abgespeichert ist. Diese Hashes können dann für den Zugriff auf andere Systeme mit demselben lokalen Passwort verwendet werden – eine häufige Fehlkonfiguration in Unternehmen. Anschließend werden Domänenkonten und weitere Systeme angegriffen (Abbildung 2). So springen die Angreifer von System zu System und lesen die Hashes der Benutzerkonten aus, die in den Systemen angemeldet sind. Dieser Prozess wird so lange fortgeführt, bis der Angreifer den Hash eines Domänen-Accounts findet, der erhöhte Berechtigungen besitzt.

Keine Angriffsfläche bieten

Das Microsoft Cyber Security Team hat festgestellt, dass die meisten untersuchten Angriffe auf dem PtH-Verfahren beruhen.

Unternehmen sollten deshalb

- hoch privilegierte Domänenkonten beschränken und schützen,
- lokale, administrative Konten beschränken und schützen sowie
- den eingehenden Datenverkehr mit der Windows-Firewall einschränken.

Eine häufige Fehlerquelle ist eine undifferenzierte Sicherheitskonfiguration der Systeme. Wesentlich effektiver ist es, eine Strategie zu entwickeln, die wichtige Entitäten wie Admin-Konten und hoch berechtigte Servicekonten umfassend absichert und weniger gefährdete Systeme nicht mit mehr Aufwand schützt als nötig.

Privilegierte Domänenkonten umfassend schützen

Häufig wird es den Benutzern administrativer Domänenkonten erlaubt, sich sowohl auf Domänen-Controllern (DC) als auch an Arbeitsplatzsystemen als „einfacher" Benutzer anzumelden. Diese Arbeitsplatzsysteme sind jedoch aufgrund der Internet-Nutzung sowie der Verwendung von Maildiensten zahlreichen Bedrohungen ausgesetzt.

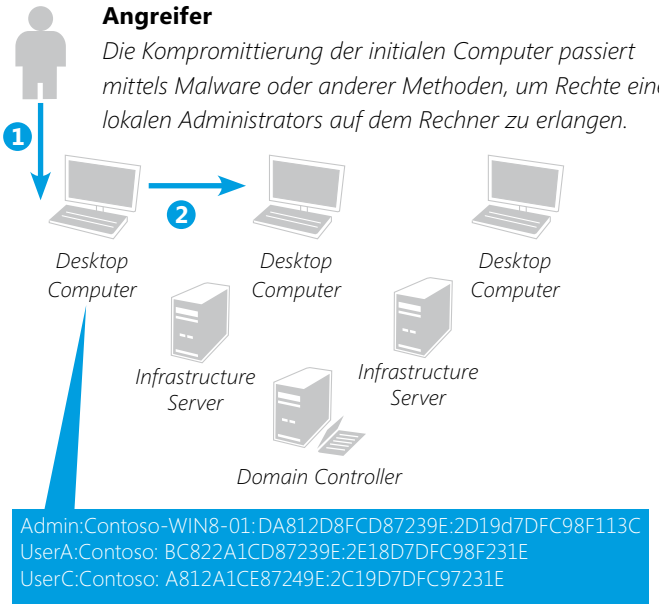
Um dieses Risiko zu minimieren, sollten

- Administratoren und andere Nutzer hoch privilegierter Konten sich ausschließlich an vertrauenswürdigen Systemen anmelden dürfen.
- Administratoren separate Konten für die tägliche Arbeit nutzen.
- administrative Aufgaben von separaten und besonders geschützten Systemen ausgeführt werden.
- hoch privilegierte Konten als „sensitiv, kann nicht delegiert werden" im Active Directory (AD) markiert werden.
- keine Dienste über administrative Domänenkonten laufen.

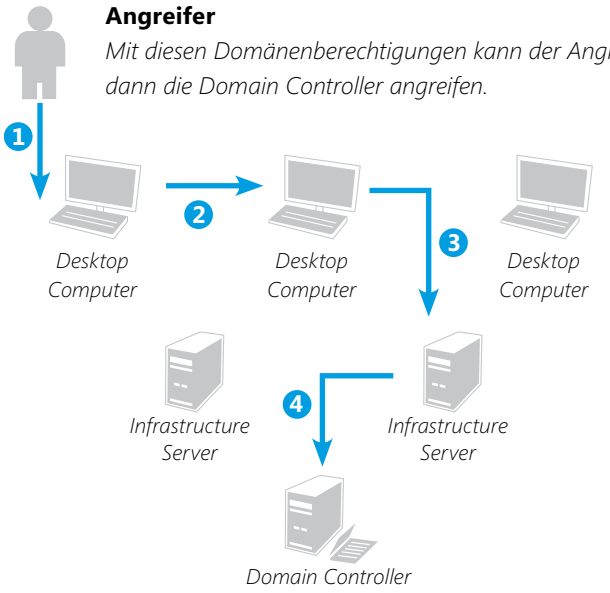
Werden die Domänenkonten nie auf kompromittierten Systemen verwendet, ist sichergestellt, dass Angreifer die Kontodaten nicht stehlen können. Die Microsoft Consulting Services bieten Lösungspakete an, die Sie dabei unterstützen, Ihre IT-Infrastruktur auf Angriffe zu untersuchen. Zudem können Unternehmen proaktive und reaktive Dienste nutzen, um Angreifer wieder aus ihrem Netzwerk zu entfernen und das Risiko einer Kompromittierung zu reduzieren. ■

Lars Klinghammer ist Security Consultant und verantwortet in seiner Rolle Security-Projekte mit nationalen und internationalen Großkunden der Wirtschaft und des Öffentlichen Dienstes. Er besitzt folgende Zertifizierungen: CISSP, ISSAP, CISA, CISM und CIPP/US.

Auslesen der Hashes aus der lokalen SAM-Datenbank
Abb. 1



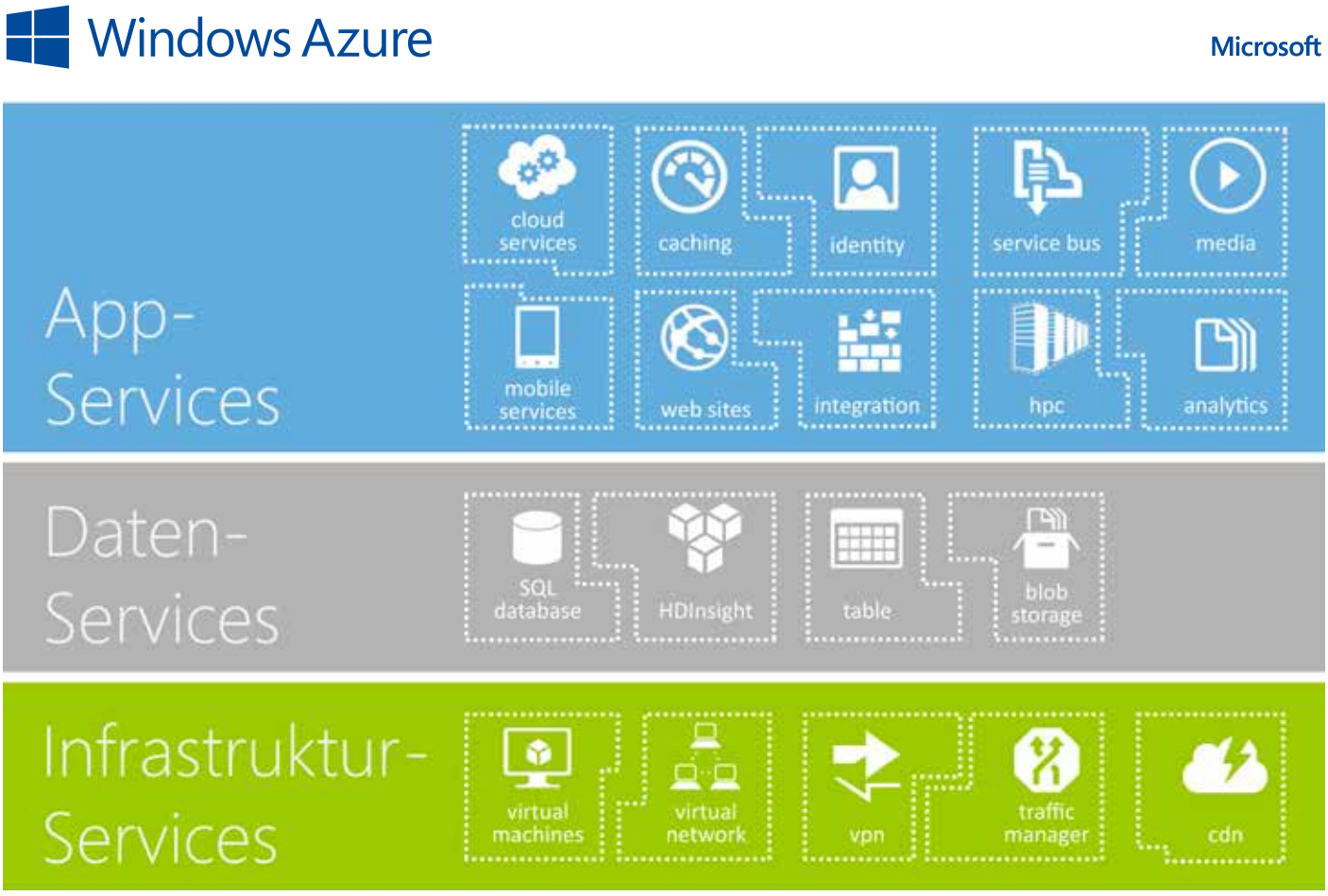
Erweiterung der Rechte über privilegierte Domänenkonten
Abb. 2



Die Cloud-Plattform für moderne Unternehmen

Unbegrenzte Möglichkeiten mit Windows Azure

Windows Azure ist eine offene und flexible Cloud-Plattform, die es ermöglicht, Infrastrukturen und Anwendungen in einem globalen Netzwerk von Microsoft-Rechenzentren schnell und effizient aufzusetzen, zu betreiben und zu verwalten. Dabei hat der Schutz der Kundendaten höchste Priorität. Microsoft setzt hierfür auf modernste Technologien und ergreift alle Maßnahmen, um maximale Sicherheit und umfassenden Datenschutz zu gewährleisten sowie alle Compliance-Vorgaben zu erfüllen.



Überblick über die Windows Azure Services

Die Microsoft Global Foundation Services betreiben die Rechenzentren, in denen die Windows Azure Services bereitgestellt werden. Dieser Geschäftsbereich von Microsoft kümmert sich um alle Prozesse rund um innovative, nachhaltige, kosteneffiziente sowie hochverfügbare Ressourcen und bedient mit Diensten wie Windows Azure, Bing, Hotmail, MSN, Office 365 und Xbox Live heute mehr als eine Milliarde Kunden und zwanzig Millionen Unternehmen in über 76 Märkten weltweit.

Sicherheit und Zuverlässigkeit garantiert

Die Microsoft-Rechenzentren liegen geografisch voneinander getrennt und erfüllen die wichtigsten Standards wie ISO/IEC 27001:2005, um Sicherheit und Zuverlässigkeit zu gewährleisten. Neben den umfassenden, physischen Sicherheitsmechanismen für Rechenzentren, Netzwerke und Mitarbeiter bietet Windows Azure auch Sicherheitsverfahren auf Anwendungs- und Plattformebene, um die Sicherheit für Anwendungsentwickler und Dienstadministratoren zu verbessern. Zudem führt Microsoft regelmäßig Tests und Prüfungen durch, um die Sicherheitsmechanismen und -prozesse in Windows

Azure zu optimieren. Eine besonders bedeutende Komponente im Produkt- und Servicelebenszyklus von Microsoft ist der Datenschutz. Das Unternehmen geht mit seinen Maßnahmen transparent um und verwaltet alle Daten äußerst verantwortungsbewusst. So dient die Datenschutzerklärung zu Windows Azure beispielsweise als Leitlinie für Kunden und erläutert die spezifischen Richtlinien für die Nutzung von Windows Azure.

Die Wahl des Standorts für die Datenspeicherung

Kunden von Windows Azure können wählen, in welchem Microsoft-Rechenzentrum oder welchen Microsoft-Rechenzentren sie ihre Daten speichern möchten. Die möglichen Länder und Regionen für die einzelnen Windows Azure-Dienste sind auf der Webseite zu Windows Azure gelistet. Aus Gründen der Datenredundanz behält sich Microsoft vor, die Kundendaten an einen anderen Ort innerhalb einer geografischen Region (z. B. innerhalb Europas) zu übertragen. So werden Blob- und Tabellendaten zum Beispiel zwischen zwei Teilregionen mit derselben Hauptregion repliziert, um im Fall einer Katastrophe Datensicherheit gewährleisten zu können. Microsoft überträgt keine Kundendaten an Standorte außerhalb der geografischen Hauptregion(en), die der Kunde auswählt – es sei denn, es wäre erforderlich, um Kundensupport bereitzustellen, ein Problem mit dem Dienst zu beheben, rechtliche Bestimmungen einzuhalten oder wenn der Kunde eine Übertragung der Daten bei der Konfiguration des Kontos aktiviert.

Gesetzliche und vertragliche Grundlagen

Microsoft hat sich dazu verpflichtet, die „Safe Harbor Principles" der Europäischen Kommission zu beachten, und ist auf der entsprechenden Liste des US-Handelsministeriums eingetragen. Damit ist gewährleistet, dass Microsoft die strengen Datenschutzgesetze der EU einhält und personenbezogene Daten aus der EU für eine Bearbeitung rechtmäßig an Orte außerhalb der EU übertragen darf. Darüber hinaus macht Microsoft Volumenlizenzkunden weitere vertragliche Zugeständnisse: Im Rahmen eines Enterprise Agreements ist es für Kunden und Partner, die Lösungen auf Windows Azure anbieten oder einsetzen, möglich, eine zusätzliche Datenverarbeitungsvereinbarung sowie Modellklauseln für EU-Verträge zu schließen. Microsoft erfüllt die Datenschutzgesetze, die im Allgemeinen für die Bereitstellung einer Cloud-Services-Plattform gelten. Dennoch liegt es in der Verantwortung der Kunden, zu entscheiden, ob Windows Azure und die jeweiligen Anwendungen, die auf der Plattform Windows Azure ausgeführt werden sollen, die Gesetze und Bestimmungen für die jeweilige Branche und das jeweilige Verwendungsszenario erfüllen. Microsoft stellt Windows Azure-Kunden detaillierte Informationen zu den Sicherheitskompatibilitätsprogrammen zur Verfügung, um diese Bewertung zu unterstützen. Zudem strebt das Unternehmen für Windows Azure unter anderem die jährliche Zertifizierung nach ISO/IEC 27001:2005 durch die British Standards Institution (BSI) sowie die jährliche Attestierung von SSAE 16/ ISAE 3402 an. ■

Weiterführende Informationen rund um das Thema Sicherheit, Datenschutz und Compliance finden Sie auf der Website zu Windows Azure:
http://www.windowsazure.com/de-de/support/trust-center/

Maria Wastlschmid ist Produkt Marketing Manager für Windows Azure in der Server, Tools und Cloud Business Group. Sie verantwortet innerhalb des Lösungsportfolios von Windows Azure den Bereich Infrastructure as a Service. Darüber hinaus ist sie in Deutschland Beauftragte für Data Privacy & Compliance im Rahmen von Windows Azure.

Microsoft

Mobiles Arbeiten ohne Grenzen

Umfassende und sichere Geräteverwaltung

Mit Windows Intune können Unternehmen sowohl firmeneigene als auch im Privatbesitz befindliche mobile und stationäre Geräte zentral verwalten und schützen. Dabei können Unternehmen zwischen einer reinen Cloud-Lösung und einer Kombination aus cloudbasierenden und vor Ort bereitgestellten Funktionen mit System Center 2012 Configuration Manager wählen.

Heutige Herausforderungen

Benutzer

Benutzer erwarten, **von überall aus arbeiten** zu können und Zugriff auf alle ihre Arbeitsressourcen zu haben.

Geräte

Die **explosionsartige Zunahme von Geräten** unterläuft den auf Standards basierenden Ansatz der Corporate-IT.

Anwendungen

Die **plattformüber-greifende** Bereitstellung und Verwaltung von Anwendungen ist schwierig.

Daten

Benutzer müssen produktiv bleiben – unter **Beibehaltung der Compliance** sowie der gleichzeitigen **Verringerung von Risiken.**

Ob Mitarbeiter aus dem Vertrieb oder Außendienst, Servicemitarbeiter oder Manager – sie alle haben eines gemeinsam: Sie arbeiten auch unterwegs und müssen stets mobil erreichbar sein. Und das, ohne dabei Produktivität einzubüßen. Damit sind auch die Anforderungen an die IT klar definiert: Diese Nutzer müssen in der Lage sein, schnell und flexibel auf Unternehmensdaten zugreifen oder spezifische Unternehmensanwendungen nutzen zu können. Microsoft schafft mit Windows Intune die Voraussetzungen, um die Geschäftsprozesse dieser Mitarbeiter effizient, produktiv, anwenderfreundlich und dennoch sicher zu gestalten.

Microsofts benutzerorientierte Geräte-Managementlösung vereint marktführendes PC-Management und mobiles Gerätemanagement. Die kommende Version von Windows Intune und System Center 2012 R2 Configuration Manager bietet IT-Verantwortlichen zahlreiche neue Funktionen, um ihre Desktop-Infrastruktur noch flexibler und sicherer zu betreiben. Sie ermöglicht Benutzern Zugriff auf Unternehmensressourcen mit dem Gerät ihrer Wahl, wobei die bestehende IT-Infrastruktur genutzt wird. Anwendungen werden in einer auf das jeweilige Gerät optimierten Art und Weise verteilt. Die IT kann sowohl unternehmenseigene als auch im Privatbesitz befindliche Geräte mit einer einheitlichen Infrastruktur verwalten, wobei Administratoren die Einhaltung von Compliance- und Unternehmensrichtlinien über eine einzige Verwaltungskonsole gewährleisten können.

Die neuen Funktionen und Vorteile im Überblick

Die nächsten Versionen von System Center 2012 R2 Configuration Manager, Windows Server 2012 R2 und Windows Intune bieten Unternehmen eine Reihe leistungsfähiger Funktionen, um „Consumerization of IT" und damit ein flexibles Arbeiten zu ermöglichen. Hierzu zählen die Möglichkeiten für Benutzer, einen konsistenten Zugriff auf Unternehmensressourcen über verschiedene Geräte zu erhalten, erweiterte Konfigurationseinstellungen für Windows-, iOS- und Android-Geräte sowie ein nahtloser und geschützter Zugriff auf interne Anwendungen und Daten aus der Cloud.

Mobile Device Management (MDM): Mobile Geräte und „Bring-your-own-Devices" werden mit Windows Intune MDM zentral verwaltet.

Device-Management-Richtlinien: IT-Administratoren können geräte- und plattformspezifisch Konfigurationsrichtlinien definieren und bereitstellen, um die Einhaltung von Compliance-Anforderungen sicherzustellen.

Selective Wipe: Sensible Unternehmensdaten werden mit Selective Wipe auf privaten Devices ausschließlich mit EFS-Verschlüsselung gespeichert. Verlässt ein Mitarbeiter das Unternehmen, wird der Schlüssel gelöscht, und die Daten auf dem Privatgerät sind unbrauchbar.

Unternehmensportal: Ein Self-Service-Portal, das auf jedem Gerät läuft, ermöglicht es Benutzern, Unternehmensanwendungen, die von der IT-Abteilung bereitgestellt werden, zu installieren. Nutzer können sich in diesem Portal einen Überblick über ihre Geräte verschaffen und diese auf Wunsch auch entfernen. Zudem können sie über das Portal die Synchronisation ihrer Arbeitsdaten anstoßen.

Work Folders: Mit dieser Funktion können Nutzer ihre Daten aus ihren Benutzerordnern des Unternehmensnetzwerks mit ihrem Gerät synchronisieren und umgekehrt.

Workplace Join: IT-Abteilungen können damit den Zugriff auf Unternehmensressourcen noch individueller und differenzierter gestalten und so sensible Unternehmensdaten effektiver absichern.

Windows To Go: Eine vollständige und verwaltete Windows 8-Desktopumgebung kann via USB-Stick bereitgestellt werden – inklusive firmeneigenem Windows-Image, spezifischen Apps, Einstellungen und Unternehmensdaten.

Windows Defender: Windows 8.1 überwacht das Netzwerkverhalten von Schadsoftware, um das Ausführen von bekannter und unbekannter Malware zu erkennen und zu stoppen.

Weitere Informationsquellen

Informationen sowie Best Practices im TechNet: http://technet.Microsoft.com/de-de/windows/intune

Kostenfreie 30-Tage-Testversion: http://www.Microsoft.de/tryintune

Assigned Access: Mit diesem neuen Feature kann eine Single Windows Store App Experience auf dem Device aktiviert werden – beispielsweise eine Kundendienst-App oder Point of Sale (POS)/Point of Interest (POI)-App.

Auto-triggered VPN: Einzelne Apps sind mit dieser Technologie in der Lage, explizit eine Verbindung per VPN anzufordern – Nutzer können sich mit nur einem Klick einloggen. ■

Manuela Pemp verantwortet in der Server, Tools und Cloud Business Group als Product Manager People-Centric IT, die Microsoft-Lösung für eine umfassende Benutzer- und Geräteverwaltung. Dies umfasst die Produkte System Center Configuration Manager, Windows Intune und Windows Remote Desktop Services.

IT-Compliance & IT-Governance

Regulatorische Anforderungen erfolgreich umsetzen

Schritt für Schritt zum IT-Compliance-Management

Zahlreiche Stellen – von Behörden über Kooperationspartner und Kunden bis hin zu internen Ansprechpartnern – fordern ein hinreichendes IT-Compliance-Management. Eine systematische und schrittweise Vorgehensweise bei der Einführung eines IT-Compliance-Management-Systems bildet den Grundpfeiler und ist die optimale Basis für kontinuierliche Verbesserungen und dauerhafte Rechtssicherheit und Richtlinienkonformität.

Der Begriff „IT-Compliance" ist nicht gesetzlich definiert. Gemeint ist hiermit die Konformität eines Unternehmens mit IT-spezifischen „[...] gesetzlichen Bestimmungen und unternehmensinternen Richtlinien [...]"[1].Dies führt zu einer umfassenden Compliance-Verantwortung für die Geschäftsleitung und die Compliance-Verantwortlichen. Gerade mit Blick auf die möglichen, mitunter sehr einschneidenden Rechtsfolgen bei Verstößen gilt es, die Compliance-Organisation rechtskonform zu gestalten. Auch wenn ein hinreichend eingerichtetes Compliance-Management-System nicht zwingend zu einer Enthaftung von Unternehmen und Compliance-Verantwortlichen führt, so kann es jedenfalls helfen, die Haftung im Falle eines entsprechenden Verstoßes deutlich zu reduzieren.[2]

Maßgebliche Anforderungen an Unternehmen und Organisationen

Da ein hinreichendes IT-Compliance-Management von hoher Bedeutung für Unternehmen und Unternehmensverantwortliche ist, stellt sich zunächst die Frage nach den maßgeblichen Anforderungen.

Maßstabsbildend sind zunächst die allgemein gesetzlichen Anforderungen. Entsprechend setzt ein hinreichendes Compliance-Management zuallererst voraus, dass sich das Unternehmen seiner entsprechenden allgemeinen Rechtspflichten bewusst ist. Hierzu zählen auf nationaler Ebene beispielsweise handels- und steuerrechtliche Pflichten, wie sie etwa aus dem HGB, der AO oder den GoBS folgen. Daneben können je nach Unternehmen weitere nationale und auch internationale Pflichten bestehen, wobei dies wesentlich von der Branche des Unternehmens abhängig ist. Datenschutz und Informationssicherheit sind mittlerweile rechtsordnungsübergreifend zu beachten, wenngleich die deutschen Anforderungen insoweit zumeist den Benchmark bilden. Dies zeigt auch der aktuelle Entwurf einer Europäischen Datenschutzgrundverordnung[3], dem zahlreiche deutsche Bestimmungen Vorbild waren[4] und der im Falle seiner Umsetzung auf gesamteuropäischer Ebene den Datenschutz daher verschärfen dürfte.

Daneben können branchen- oder unternehmensspezifische Regelungen zu beachten sein. Teilweise werden diese, wie etwa das Beispiel eines Code of Conduct zeigt, erst nach einer Selbstverpflichtung bindend. Exemplarisch sind insoweit die Verhaltensregeln für die Datenverarbeitung in der Versicherungsbranche zu nennen, die erst nach einer entsprechenden Beitrittserklärung branchenspezifische Datenschutzpflichten auslösen. Auch Standards können für ein Unternehmen verpflichtend sein. Hat sich etwa ein Unternehmen dazu entschlossen, ein standardisiertes Informationssicherheitsmanagementsystem („ISMS"), beispielsweise nach ISO/IEC 27001 oder BSI-Grundschutz, zu implementieren, muss es die standardgemäßen Anforderungen auch erfüllen. Selbstverständlich muss ein Unternehmen auch sicherstellen, dass alle sonstigen internen (insbesondere Richtlinien und Arbeitsanweisungen) und externen IT-spezifischen Regelungen (beispielsweise aus Lizenz-, Vertrags- und Fernabsatzrecht) beachtet werden. Dies

macht deutlich, dass Monitoring und ständige Verbesserungsmaßnahmen wesentliche Bestandteile eines ordnungsgemäßen IT-Compliance-Managements sind.

Aufbau eines IT-Compliance-Management-Systems

Es empfiehlt sich, systematisch und schrittweise vorzugehen und idealerweise auf bereits vorhandene Strukturen zur IT-Governance aufzubauen.[5] Unternehmen sollten dabei berücksichtigen, dass sich ein IT-Compliance-Management-System aus den Komponenten

- übergeordnete Rahmenbedingungen (z. B. Richtlinien)
- Menschen (z. B. Schulungsmaßnahmen und Verhaltensregeln)
- Technologie (z. B. technische Infrastruktur) sowie
- Prozesse und Organisation (z. B. Change Management)

zusammensetzt.

Um Komponenten und Anforderungen handhabbar zu machen, empfiehlt es sich, nach Themengebieten (z. B. Informationssicherheit, Datenschutz, Business Continuity) vorzugehen, wobei die Maßnahmen widerspruchsfrei sein müssen und Synergien genutzt werden sollten. Der systemische Charakter des IT-CMS ist durch eine zyklische und anlassbezogene Evaluierung der Rahmenbedingungen sowie eine stetige Überprüfung des Umsetzungserfolgs bereits ergriffener Maßnahmen (Plan, Do, Check, Act) sicherzustellen. So ist eine kontinuierliche Verbesserung der Compliance gewährleistet, was mit den Überwachungspflichten von Geschäftsleitung und Compliance-Verantwortlichen unmittelbar korrespondiert.

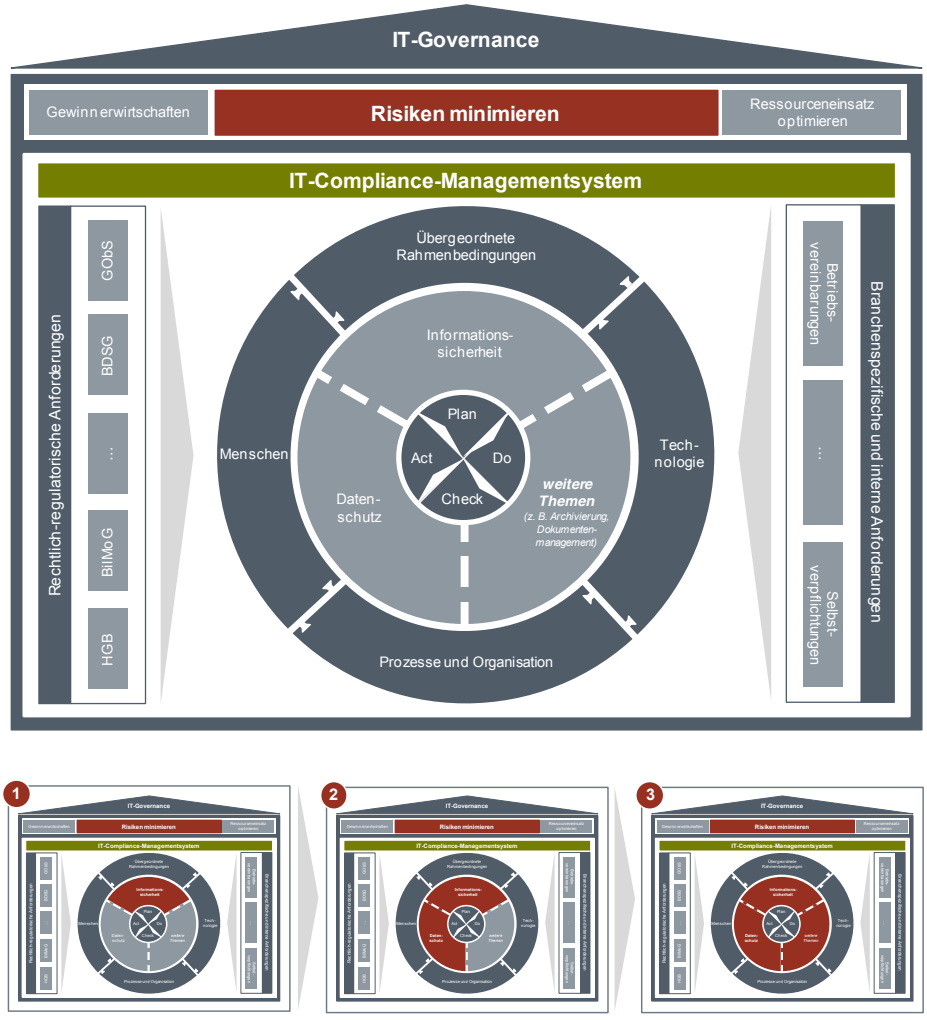
Es empfiehlt sich, in der Praxis mit dem Aufbau eines standardisierten ISMS (etwa nach ISO 27001) zu beginnen und weitere Systemkomponenten, wie das Datenschutzmanagement, im Anschluss zu ergänzen. Auf diese Weise lässt sich in der Regel eine große Anzahl an Synergien – etwa im Dokumentenmanagement und im technisch-organisatorischen Datenschutz – erzielen, Kosten lassen sich reduzieren und Widersprüche vermeiden.

Weitblick erforderlich

Um IT-Compliance-Anforderungen erfolgreich und kosteneffizient umzusetzen und alle Vorgaben zu erfüllen, ist ein systematisches Vorgehen mit Weitblick erforderlich. Dies sollte insbesondere dann berücksichtigt werden, wenn aufgrund von knappen Ressourcen oder engen Zeitfenstern eine schrittweise Umsetzung der Maßnahmen vorgesehen ist. Der schrittweise Aufbau eines IT-Compliance-Management-Systems ist hierfür eine gute Alternative. ■

Dr. Thorsten B. Behling,
Partner und Rechtsanwalt
für Datenschutz und
IT-Recht bei der WTS

Rüdiger Giebichenstein,
Partner und Experte für IT-Compliance
und Informationssicherheit
bei der WTS



IT-Compliance-Managementsystem – schrittweiser und themenbezogener Aufbau

[1] *Vgl. Regierungskommission Deutscher Corporate Governance Kodex: Deutscher Corporate Governance Kodex, online im Internet: http://www.corporate-governance-code.de/ger/download/kodex_2010/D_CorGov_Endfassung_Mai_2010.pdf, Stand 26.05.2010, S. 6.*

[2] *Vgl. Withus/Hein, Prüfung oder Zertifizierung eines Compliance Management Systems. Voraussetzungen und mögliche Rechtsfolgen, CCZ 2011, 125, 127.*

[3] *Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012), S. 11.*

[4] *Vgl. eco - Nachrichten aus der Internetwirtschaft, MMR-Aktuell 2012, 331099.*

[5] *Unter IT-Governance sind Prozesse und Organisationsstrukturen zu verstehen, die darauf hinwirken, dass die Unternehmens-IT die Erreichung der Unternehmensziele bestmöglich unterstützt.*

Mehr Sicherheit im Unternehmen

Durchblick bei der E-Mail-Archivierung

Grundsätzliche Archivierungspflichten und gesetzliche Vorgaben verunsichern Geschäftsführer, Compliance-Beauftragte und IT-Verantwortliche gleichermaßen. Wann ist eine E-Mail-Archivierung rechtssicher und was gilt es zu beachten? Verschaffen Sie sich einen Überblick.

HGB, AO und GBO, GoBS, GDPdU und TKG. Die Fantastischen Vier hätten in ihrem Song „MfG – Mit freundlichen Grüßen" den gesamten Liedtext mit den Kürzeln der Gesetzesgrundlagen für die Archivierung füllen können. Als Hersteller einer Archivierungssoftware stößt auch GWAVA immer wieder auf das Problem vielschichtiger, gesetzlicher Vorgaben. Für viele IT-Manager ist das Thema E-Mail-Archivierung einfach zu komplex und wird deshalb oftmals stiefmütterlich behandelt – ganz nach dem Motto „bevor wir etwas falsch machen, lassen wir es lieber ganz bleiben". Doch auch wenn die Gesetze und Richtlinien ein schwieriges Thema sind, lohnt sich der Einsatz einer Archivierungslösung in jedem Fall.

Wieso muss archiviert werden?

In Deutschland gibt es verschiedene Gesetze, die bei der Archivierung eine Rolle spielen. Die wichtigsten Gesetze sind dabei das Handelsgesetzbuch (HGB) und die Abgabenordnung (AO). Diese legen die grundsätzliche Archivierungspflicht fest. Hinzu kommen weitere Gesetze, die sich mit Themen wie dem Datenschutz, der Form der Aufbewahrung und den Folgen bei Missachtung der Vorschriften befassen.

Die wichtigsten Gesetze für die Archivierung elektronischer Kommunikation sind:

- Handelsgesetzbuch (HGB)
- Abgabenordnung (AO)
- Grundsätze ordnungsgemäßer Buchführung (GBO)
- Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)
- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
- Aktiengesetz (AktG)
- Gesetz betreffend die Gesellschaft mit beschränkter Haftung (GmbHG)
- Umsatzsteuergesetz (UStG)
- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG)
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Weitere hilfreiche Informationen zu diesen Gesetzen liefern unter anderem der „Verband Organisations- und Informationssysteme (VOI), die „IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnologie" oder auch Fachanwälte für IT-Recht.

Wer muss archivieren?

Art. 257 Abs. 1 des Handelsgesetzbuchs besagt, dass jeder Kaufmann Unterlagen geordnet aufbewahren muss. Unter diese Definition fallen auch Handelsgesellschaften, eingetragene Genossenschaften und juristische Personen. Hierbei ist es wichtig zu wissen, dass die Verantwortung für die Archivierung nicht bei der IT-Abteilung oder dem Compliance-Beauftragten liegt, sondern bei der Geschäftsführung beziehungsweise den Vorstandsmitgliedern (§ 93 AktG/§ 43 GmbHG). Verletzen die Verantwortlichen ihre Buchführungspflicht, drohen zivilrechtliche und strafrechtliche Konsequenzen. Diese können von Geldbußen bis hin zu Freiheitsstrafen reichen:

- § 162 AO: steuerliche Konsequenzen wie Strafzahlungen an das Finanzamt
- § 283 StGB: Verletzung der Buchführungspflicht, es drohen beispielsweise Freiheitsstrafen von bis zu zwei Jahren
- § 274 StGB: Löschung oder Abänderung von beweiserheblichen Daten können beispielsweise eine Freiheitsstrafe von bis zu fünf Jahren nach sich ziehen

Was muss archiviert werden?

Für Unternehmen gilt es, E-Mails, die Handelsgeschäfte betreffen und für die Besteuerung relevant sind, zu archivieren (§ 257 HGB/§ 140 AO). Der Inhalt der E-Mails ist somit von hoher Bedeutung und

Unified Archiving mit GWAVA

Der Einsatz einer Software für die E-Mail-Archivierung lohnt sich: Unternehmen können so nicht nur alle gesetzlichen Vorschriften erfüllen, sondern auch ihre Kosten senken und die Produktivität steigern: Dank Deduplizierung lassen sich die Speicherkosten beispielsweise um bis zu 50 Prozent reduzieren. Mitarbeiter können mit nur wenigen Mausklicks E-Mail-Nachrichten wieder auffinden oder gelöschte Nachrichten wiederherstellen – auch ohne Unterstützung des IT-Administrators. Diese und viele weitere Vorteile bietet beispielsweise die Archivierungslösung „Retain" von GWAVA. Ausführliche Informationen rund um die E-Mail-Archivierung finden Sie auf der Webseite www.Archive4All.com.

zeigt, wie komplex das Thema ist. Auf der einen Seite müssen relevante E-Mails archiviert werden, auf der anderen Seite sollten bzw. dürfen bestimmte E-Mails nicht archiviert werden – beispielsweise aus Datenschutzgründen. Eine klare Trennung ist in der Praxis oft nicht möglich. Bilanz- und steuerrelevante E-Mails wie beispielsweise Angebote müssen archiviert werden. Je nach Ermessen der Geschäftsführung sollten beispielsweise auch „relevante" E-Mails der internen Kommunikation archiviert werden. Dagegen dürfen private Mails und dienstliche Mails mit personenbezogenem Inhalt – zum Beispiel E-Mails vom Betriebsrat – nicht archiviert werden.

Wie muss archiviert werden?

Grundsätzlich können Unternehmen ihre Daten schriftlich, elektronisch oder in vergleichbarer Weise aufbewahren. Aufgrund des hohen Volumens an archivierungspflichtigen Daten ist es heute im Regelfall sinnvoll, diese Informationen elektronisch aufzubewahren. Wenn Daten elektronisch archiviert werden, muss dies entsprechend einiger Gesetze geschehen. Maßgebend sind hierfür wieder folgende Gesetze: AO, GoB, GoBS und GDPdU. Der Verband Organisations- und Informationssysteme (VOI) hat zu diesem Thema einen Leitfaden erstellt, der die wichtigsten Anforderungen an die Archivierung von elektronischer Kommunikation zusammenfasst:

- ordnungsgemäß
- vollständig (inkl. Anhängen, sozialen Medien und mobilen Daten)
- frühestmöglich
- mit Original übereinstimmend
- mit Berechtigung einsehbar
- wiederauffindbar und reproduzierbar
- Vernichtung erst nach Ablauf der Archivierungspflicht
- Protokollierung aller Änderungen im Archiv
- für einen Zeitraum von sechs bzw. zehn Jahren
- auch nach einem Systemwechsel getreu der genannten Richtlinien

Unternehmensrichtlinien definieren

Ein Großteil aller Unternehmen in Deutschland ist aufgrund der Gesetzeslage dazu verpflichtet, zu archivieren. Dabei ist es allerdings oft schwer, zwischen archivierungspflichtigen und nicht archivierungspflichtigen Daten zu unterscheiden. Hinzu kommt, dass auch die Form der Archivierung spezielle Anforderungen mit sich bringt. Hilfreich ist in jedem Fall die Festlegung von Unternehmensrichtlinien, die deutlich definieren, wie das Thema im Unternehmen gehandhabt wird. So kann beispielsweise durch eine Einverständniserklärung der Mitarbeiter die Nutzung privater E-Mails im Unternehmen unterbunden werden. Auf diese Weise lassen sich Rechtsunsicherheiten für den Arbeitgeber und den Arbeitnehmer vermeiden. ■

Christian Heselhaus,
Director Marketing &
Business Development EMEA
GWAVA EMEA GmbH

Auf dem Weg zur Personal Data Economy

Aus Daten Nutzen schaffen

Persönliche oder personenbezogene Daten stellen eine überaus wichtige Ressource dar, die dem Kapital und der Arbeit gleichzustellen ist. Sie können Innovationen fördern, neue Dienstleistungen schaffen und das Wachstum der Wirtschaft erheblich vorantreiben. Die Einhaltung gesetzlicher Vorgaben sowie die Schaffung neuer, rechtlicher Rahmenbedingungen sind die Voraussetzungen hierfür.

„Personal data will be the new ‚oil', a valuable resource of the 21st century." – dieser Satz wurde auf dem World Economic Forum in Davos geprägt.[1] Aus diesem treffenden Statement ergeben sich jedoch auch einige Fragen:

- **Was umfasst „Personal Data"?**
- **Wem gehören diese Daten?**
- **Welche Werte bilden diese Daten?**
- **Wie werden diese Werte geschützt oder sicher verwahrt?**

Auf die ersten Fragen können wir heute schon Antworten geben – zumindest teilweise. Die letzte Frage bleibt in einer sich ständig weiter mobilisierenden Welt noch lange spannend.

Was umfasst „Personal Data"?

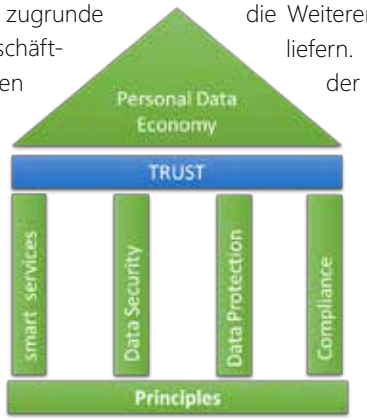
Unter „Personal Data" sind personenbezogene Daten zu verstehen. Die Richtlinie 95/46/EG der EU (Datenschutzrichtlinie) definiert den Begriff der personenbezogenen Daten für die Mitgliedsstaaten der Europäischen Union in Artikel 2 lit. a als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person'); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind". Das deutsche Bundesrecht definiert in § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Solche Daten können freiwillig oder unfreiwillig, über Aktionen, Standorte oder aus abgeleiteten Daten entstehen.

Wem gehören die Daten und wer hat welche Rechte daran?

Den meisten Menschen erscheinen diese Fragen einfach und profan, denn sie vermuten, dass sie selbst Eigentümer ihrer Daten sind und das alleinige Bestimmungsrecht über diese Daten haben. Bei genauerer Betrachtung wird jedoch klar, dass es Daten gibt, die personenbezogen sind und über die das Individuum jedoch kein Bestimmungsrecht hat. Hierbei handelt es sich beispielsweise um das Strafregister, die Daten beim Finanzamt oder bei den Krankenkassen und vieles mehr.

Die „Personal Data Economy"

Um von einer „Personal Data Economy" zu sprechen, müssen die Daten einen Wert haben. Welchen pekuniären Wert personenbezogene Daten haben, hängt von verschiedenen Faktoren ab. Hierzu zählen unter anderem die zugrunde liegenden rechtlichen, geschäftlichen und technologischen Gegebenheiten. Hinzu kommt, dass diese einem ständigen Wandel unterliegen. Um beim Ausgangsbild zu bleiben: Rohöl ist recht zäh, zum Treibstoff wird es erst nach einer Behandlung. Wie werden wir personenbezogene Daten in Zukunft behandeln, damit sie zu einem mikro- und makroökonomischen Treibstoff werden? Dass dabei die datenschutzrechtlichen Vorschriften zu beachten sind, ist selbstverständlich. Dass es auch Missbräuche geben wird, ist bedauerlich, aber sehr wahrscheinlich. Dies sollte uns jedoch nicht davon abhalten, die enormen Möglichkeiten, die eine Personal Data Economy bieten kann, zu ergreifen. Zunächst einige Beispiele:



Automobilbranche: Ein Gewerbetreibender least ein KfZ der neuesten Oberklassegeneration. Nach drei Jahren gibt er das KfZ zurück und least das Folgemodell. Welche Informationen über das Fahrverhalten von KfZ (und Fahrer) sind gespeichert? Denkbar sind z. B. Längsbeschleunigung, Querbeschleunigung, Richtungsänderung, Positionen, Licht ein- oder ausgeschaltet, Bremsenbetätigung, Blinker gesetzt oder nicht, Verbrauch, Sicherheitsgurt angelegt oder nicht etc. Zu jedem Ereignis werden Datum und Uhrzeit gespeichert. Diese Informationen gehen – auch nach Ablauf des Leasing-Vertrags – nicht unter. Es ist anzunehmen, dass sie den Automobilherstellern wichtige Informationen für die Weiterentwicklung der Fahrzeuge liefern. Datenschützer und selbst der ADAC warnen vor einem Big-Brother-Effekt. Das Thema lässt sich aber auch noch von einer anderen Warte betrachten. Was wäre, wenn unser Gewerbetreibender die Überlassung der Daten an die Automobilhersteller von einer Zahlung an ihn abhängig machen würde. Nach dem Motto: „Ich habe für dich fleißig Daten gesammelt, nun möchte ich die Früchte meines Tuns

einfahren." Viel interessanter für den Automobilhersteller und den Datensammler wäre allerdings ein anderes Modell: Der Automobilhersteller wertet die Daten der vergangenen drei Jahre für den Fahrer individuell aus und gibt ihm eine detaillierte Auswertung, z. B. welcher KfZ-Typ für ihn der ökonomischste wäre. Dafür darf er die Daten des Datensammlers anonymisiert für eigene Zwecke verwenden.

Gesundheitswesen: Die Gegenwart bedingt ein hohes Maß an Flexibilität und Mobilität in der Berufswelt. Hierzu wieder ein einfaches Beispiel. Der Sohn hat eine Stelle in München angenommen. Seine Mutter lebt in Hamburg und hat gesundheitliche Probleme, die den Sohn sorgen. Er hat ein schlechtes Gewissen, sich nicht besser kümmern zu können. Da erfährt er von einer App. Alle Informationen und Dokumentationen zu einem Patienten werden in einem Portal gespeichert. Das Fachpersonal einer Kranken- oder Pflegeeinrichtung kann die ermittelten Daten des Patienten noch während der Versorgung automatisiert an das Portal übermitteln und so dem gesamten Betreuungsnetzwerk des Patienten zur Verfügung stellen. Auch der Patient selbst kann mit Hilfe des Remote Monitorings Gesundheitsdaten wie Blutdruck, Blutzucker etc. ermitteln und diese im Portal ablegen, entweder manuell oder auch automatisiert. Die Informationen und Dokumentationen des Patienten werden u. a. von medizinischen Geräten über Bluetooth-Anbindung z. B. auf das Portal übertragen. Das Ergebnis steht dem Berechtigten sodann auf einer App zur Verfügung. Im Bedarfsfall gibt die App Alarm oder informiert bei Unter- oder Überschreiten bestimmter Werte automatisch den Arzt oder die Notrettung. Die Benutzung der App ist kostenlos. Dafür werden die Daten anonymisiert den Krankenkassen zur Verfügung gestellt. Alternativ könnte die App beispielsweise 5,00 EUR im Monat kosten und die Daten werden nicht weiter verwertet. Der Sohn bespricht die App mit seiner Mutter. Sie stimmt zu. Der Sohn ist nun immer zeitnah informiert und kann handeln. Die Familie ist glücklich. Der Datenschützer antizipiert besorgt.

Interessante Mehrwertdienste

Die Übertragung und die Verwertung von Daten werden noch einige IT-technische, juristische und ökonomische Fragen aufwerfen. Die Antworten versprechen spannend zu werden. Es wird Mahner geben, die vor dem gläsernen Menschen und eventuellen Missbräuchen warnen werden. Aufgeschlossene Datenschützer werden überlegen, ob in der Ergänzung des Datenschutzes um den Bereich Personal Data Economy nicht eine große Chance für die eigene Positionierung liegt. Und es wird diejenigen geben, die über interessante Mehrwertdienste nachdenken und sie schließlich anbieten. Das Individuum wird am Ende entscheiden, ob es diese Dienste in Anspruch nehmen wird. Dies wird nur der Fall sein, wenn das Vertrauen in die Sicherheit und Compliance professionell aufgebaut ist und als glaubhafte Elemente wahrgenommen werden. ■

Dr. Hanns Suckfüll,
Geschäftsführer
HSBD GmbH

Association for Personal Data Economy

Der Verband „Association for Personal Data Economy" hat den Zweck, die Zusammenarbeit zwischen Wissenschaft und Praxis auf dem Gebiet der mit dem internationalen und insbesondere europäischen Datenschutz in Einklang stehenden Datenverwertung zu fördern – insbesondere in den Bereichen Energie, Mobilität, Kommunikation, Industrie, Gesundheitswesen und anderen Themenfeldern, die personenbezogene und verwertbare Daten betreffen. Weitere Informationen finden Sie unter www.apde-org.eu.

[1] *http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf*

Compliance-Anforderungen abdecken und unternehmerischen Mehrwert schaffen

IAM-Projekte erfolgreich umsetzen

Die Planung, die Umsetzung und der Betrieb einer IAM-Lösung stellen Unternehmen vor viele Herausforderungen. Sie müssen Prozesse definieren und standardisieren und zahlreiche Compliance-Vorgaben einhalten, um ihre gesamte Infrastruktur und ihre Anwendungen einheitlich und nachvollziehbar verwalten zu können. Die Oxford Computer Group ist Spezialist für Identity und Access Management und zeigt, wie ein IAM-Projekt zielgerichtet und erfolgreich umgesetzt werden kann.

Nationale gesetzliche Vorgaben, internationale Regelungen und unternehmensspezifische Richtlinien haben heute zunehmenden Einfluss auf die flexible Bereitstellung von Ressourcen für die Geschäftsprozesse innerhalb eines Unternehmens. Systeme für Identity & Access Management (IAM) können Sie dabei unterstützen, diese Prozesse zu standardisieren und Vorgaben und Regelungen unternehmensweit einzuhalten. Experten definieren IAM als Richtlinien, Prozesse und Systeme, die effektiv steuern und verwalten, wer in einer Organisation wann Zugriff auf welche Informations- und Datenquellen hat.[1]

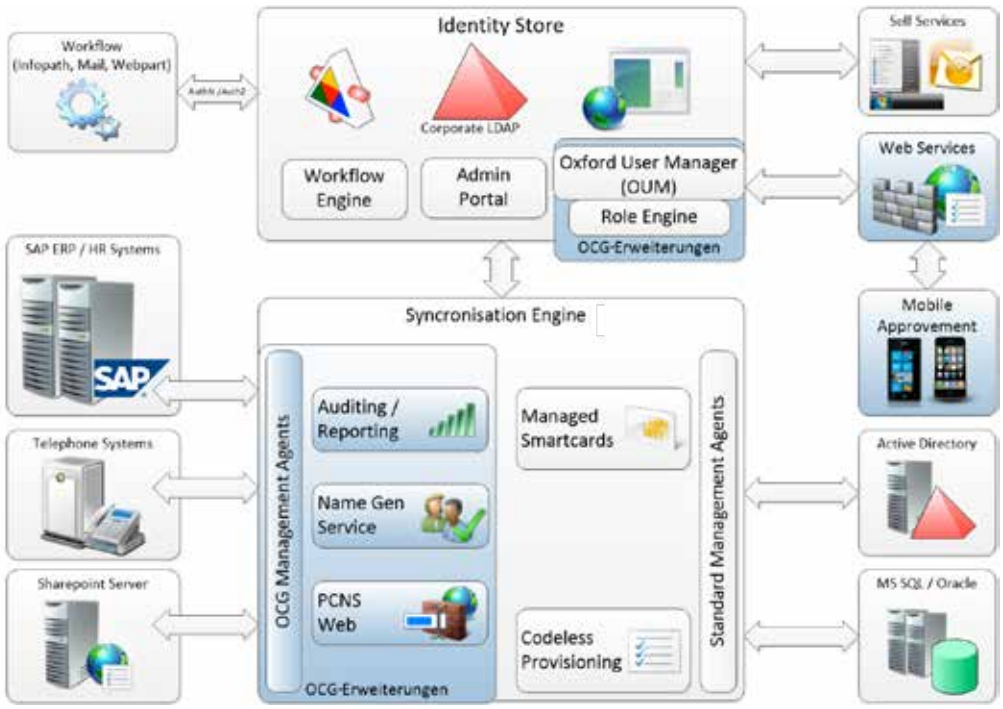
Schutz der IT-Systeme und des geistigen Eigentums

IT-Verantwortliche nehmen heute die „interne Bedrohung" ihrer IT-Infrastruktur ebenso ernst wie die Bedrohungen von außen durch Malware oder Cyberkriminelle. Während die Absicherung nach außen inzwischen einen hohen Grad an Professionalisierung erfahren hat, setzt eine Vielzahl an Unternehmen für die Absicherung nach innen oftmals noch einzelne, systemspezifische Lösungen ein. Fehlende Zugriffsregelungen, verwaiste Benutzerkonten und die mangelnde Nachvollziehbarkeit von Berechtigungen stehen im Widerspruch zu der für Unternehmen

[1] *KPMG IT Advisory*

IAM-Gesamt-Architektur

(ergänzt durch OCG-Softwaremodule)



- Zentrale webbasierte Benutzeradministration
- Mächtige Workflow Engine
- Passwort-Synchronisation
- Passwort-Reset-Portal
- Outlook-Integration
- Integriertes Zertifikats-management (Smartcard)
- ADFS-Integration (SAML)
- > 100 weitere System-Anbindungen verfügbar

Oxford User Manager (OUM)

- Darstellung/Management von Business-Strukturen
- Optional: Integriertes RBAC-Modul

Audit & Reporting Solution

- Audit/Reporting über SSRS und OCG Reporting Tool

immer wichtiger werdenden Umsetzung von Compliance-Anforderungen, die der Sicherung der IT-Infrastruktur dienen.

Komplexität beachten

IAM-Konzepte und das damit einhergehende zentrale Management von IT-Ressourcen unterstützen Unternehmen dabei, die Informationsverarbeitung zu standardisieren und angeschlossene Systeme einheitlich und nachvollziehbar zu verwalten. Dabei sollten Unternehmen beachten, dass hierbei sehr schnell sehr komplexe Systeme entstehen, die erhebliche Ressourcen innerhalb der IT-Abteilung eines Unternehmens binden können.

Die Gründe hierfür sind:

- sehr unterschiedliche und komplexe Anforderungen an ein IAM-System,
- die erforderliche zeitnahe Verarbeitungsgeschwindigkeit der Anforderungen sowie
- ein hoher Dokumentationsaufwand, um die Transparenz der abgebildeten Prozesse sicherzustellen.

Im internationalen Umfeld können technische oder auch kulturelle Schwierigkeiten dazu führen, dass IAM-Projekte noch komplexer werden. Dynamisch geplante IAM-Projekte ermöglichen es, Teilprojekte flexibel zu realisieren und bereits frühzeitig einen wirtschaftlichen Mehrwert zu schaffen.

Compliance-Anforderungen erfüllen

Compliance-Anforderungen sind heute ein wichtiger, aber nicht der alleinige Treiber für die Implementierung von IAM-Systemen. Die Vielzahl gesetzlicher Regelungen, u. a. Sarbanes Oxley Act, Basel II, KontraG, Bundesdatenschutzgesetz (BDSG), beziehen sich zwar nicht direkt auf die IT, haben aber einen unmittelbaren Einfluss auf die Planung eines IAM-Systems, da sie beispielsweise eine direkte, transparente und fehlerfreie Nachvollziehbarkeit von Prozessen in Form von Berichten fordern. Zudem ist die Umsetzung von Compliance-Vorgaben eine wichtige Voraussetzung, um Audits erfolgreich durchzuführen.

Informationssicherheit gewährleisten

Die Speicherung und die Verarbeitung von personenbezogenen Daten unterliegen strengen Vorgaben und Richtlinien. Diese Daten dürfen nur berechtigten Benutzern zugänglich gemacht werden. Dies gilt jedoch oftmals auch für unternehmensinterne Informationen. IAM-Systeme ermöglichen es, diese Daten standardisiert und transparent zu verarbeiten, und schaffen damit auch eine höhere Sicherheit. Zudem vereinfacht eine einheitliche und nachvollziehbare Verarbeitung die Risikoeinschätzung für das IT-System oder die IT-Infrastruktur.

Offene Systeme als Herausforderung

Vernetzte Geschäftsprozesse binden heute Kunden, Lieferanten oder auch Vertriebspartner in die Infrastruktur ein (Identity Federation). Dies führt unweigerlich zu einer Öffnung der IT-Infrastruktur nach außen. Web-Services und serviceorientierte Architekturen forcieren diese Entwicklung zusätzlich. In Konsequenz ist die Verwaltung der Zugriffe Dritter auf interne IT-Ressourcen eine große Herausforderung für Unternehmen, die eine IAM-Struktur implementieren. Die Nachvollziehbarkeit von IAM-Prozessen ist insbesondere aus Gründen der Haftung von großer Bedeutung.

Die IAM-Strategie als Schlüssel zum Erfolg

Die einheitliche und durchgängige Konzeption einer IAM-Lösung bildet die Basis für die erfolgreiche Implementierung und Umsetzung. Hierbei ist es wichtig, nicht nur die passende IAM-Lösung auszuwählen, sondern auch darauf zu achten, dass diese Software umfassende, unternehmensspezifische Anpassungen ermöglicht. Unternehmen sollten zudem bereits vorhandene Lösungen oder Lösungskomponenten in ihrer IT-Infrastruktur im Vorfeld analysieren und – falls diese nicht im Widerspruch zur Gesamtkonzeption stehen – in die systemübergreifende IAM-Struktur integrieren.

Die Entwicklung einer IAM-Strategie sollte folgende Schwerpunkte setzen:

- Authentifizierungsverfahren für angeschlossene Systeme
- Rechteverwaltung für angeschlossene Systeme
- Widerspruchsfreie Berichte
- Definition von Verantwortlichkeiten für Prozesse. ■

Die Oxford Computer Group GmbH – das Unternehmen, die Leistungen

Die Oxford Computer Group GmbH (OCG) verfügt über langjährige Erfahrung bei der umfassenden Planung und der methodischen Umsetzung von IAM-Projekten auf Basis von Microsoft-Technologien. OCG unterstützt Unternehmen dabei, Machbarkeitsstudien (Proof-of-Concept) bei der Planung und Durchführung zu realisieren. Dank der von OCG entwickelten Tools ist es möglich, verschiedene Systeme schnell und unkompliziert zu verbinden und deren Informationen zum Nachweis der technischen Machbarkeit zu verarbeiten. Die OCG verfügt zudem über umfassendes Know-how bei der Umsetzung von gesetzlichen Vorgaben und bei der Entwicklung und Implementierung unternehmensspezifischer Vorgaben und Richtlinien. Das Unternehmen legt bei der Ausrichtung der Gesamtstrategie großen Wert auf eine prozessorientierte IAM-Strategie, um ein hohes Maß an Flexibilität zu erreichen. Das übergeordnete Ziel aller Maßnahmen der IAM-Strategie ist es, den unternehmerischen Fokus in die IAM-Strategie mit einzubeziehen und einen geschäftlichen Mehrwert zu schaffen.

Ihr Ansprechpartner bei OCG: Daniela Eis, Program Manager, Oxford Computer Group GmbH, www.oxfordcomputergroup.de

Andreas Bünseler,
Consultant
Oxford Computer Group GmbH

Die Harmonisierung von Technik und Prozessen schafft Compliance

Daten- und Dokumentenmanagement über Systemgrenzen hinweg

Daten- und Dokumentenaustausch über Systemgrenzen hinweg ist insbesondere im regulierten Umfeld der Pharmaindustrie eine Herausforderung. Microsoft und Alegri International bieten Lösungen an, diese hohen Anforderungen effizient und regelkonform umzusetzen.

Steigender Effizienzdruck und eine immer stärkere Regulierung des Marktes für Pharmaprodukte führten zu zwei Entwicklungen: Verschiedene Aufgaben der Wertschöpfungskette werden an externe Dienstleister und Partner vergeben. Hierzu zählen beispielsweise klinische Studien, Forschungsaufträge, Lohnherstellung, IT-Systeme und deren Betreuung. Parallel dazu konzentrieren sich Pharmahersteller wie auch Dienstleister darauf, FDA- und GMP-konforme, computergestützte Systeme einzuführen und zu nutzen. Im Mittelpunkt stehen hierbei die Erfassung, Verarbeitung und der Austausch gemeinsam genutzter Daten und Dokumente. Es gilt, das Zusammenspiel der unterschiedlichen Partner über IT-Systeme hinweg abzubilden und zugleich die hohen Anforderungen an deren Qualifizierung sowie die Validierung der auf ihnen abgebildeten Prozesse zu erfüllen.

Alegri International Group
Alegri ist ein führendes IT-Beratungsunternehmen im Bereich aller Microsoft-Produkte, inkl. SAP-Integration und Prozessoptimierung. Durch diese Spezialisierung beherrscht Alegri als Enterprise-Architekt das Zusammenspiel der Applikationen über alle unternehmerischen Prozesse hinweg: SharePoint mit Search, Dynamics CRM, Lync/Exchange, Duet, System Center, Office 365/Azure, .Net, SQL Server.
Alegri wurde 2001 gegründet und beschäftigt heute rund 290 Mitarbeiter an zehn Geschäftsstandorten: München, Stuttgart, Mannheim, Frankfurt/M., Köln, Hamburg, Wien, Basel, Zürich, Cluj-Napoca.
www.alegri.eu

Im Spannungsfeld zwischen Wirtschaftlichkeit und Compliance

Von der Erforschung neuer Medikamente, den für ihre Zulassung notwendigen klinischen Studien, der Zulassung selbst und dem gesamten Produktionsprozess – IT-Systeme sind hierbei nicht mehr wegzudenken. Eine Herausforderung ist die Heterogenität der IT-Infrastrukturen der an diesen Aufgaben beteiligten Pharmaunternehmen, Dienstleister und Partner. Selbst wenn Daten bereits elektronisch übertragen werden, fehlt über die Systemgrenzen hinweg ein gemeinsamer Ansatz zur Automation, beispielsweise über Workflows.

Dies zieht die Verwendung unterschiedlicher Frontends und Tools sowie gegebenenfalls manuelle Schritte nach sich. Ein großer Teil der Daten und Dokumente unterliegt den strengen Regularien der Zulassungsbehörden. Das bedeutet für die zugrundeliegenden IT-Systeme eine Qualifizierung und Validierung, die mit US FDA 21 CFR Part 11 oder EU GMP Annex 11 konform ist.

Aufgrund der Medienbrüche, der teils notwendigen händischen Eingriffe in die Daten- und Informationsflüsse sowie der Anzahl heterogener Systeme steigt der Qualifizierungs- und Validierungsaufwand für Erreichung und Erhalt der Compliance. Im Hinblick auf eine wirtschaftlich effiziente Einführung von IT-Systemen in diesem Umfeld empfehlen sich zwei Wege:

- zentrale, plattformgestützte Systeme, die als Orchestrierungssoftware fungieren können, ermöglichen eine konsequente Harmonisierung
- Unternehmen sollten effiziente und pragmatische Ansätze für die Qualifizierung und Validierung dieser Systeme einführen und nutzen

Daten und Dokumente zentral verwalten

Mit der Microsoft SharePoint-Technologie steht eine Plattform zur Verfügung, die den gesamten Daten- und Dokumenten-Lifecycle in Form prozessbezogener Workflows auch über Systemgrenzen hinweg abbilden kann. Alegri International hat auf Basis von SharePoint ein FDA-/GMP-konformes eDMS entwickelt, das die Anforderungen an Audit-Trails, elektronische Signatur und Langzeitarchivierung erfüllt und sich auch in verschiedene Backend-Systeme der Unternehmen integrieren lässt: Verwaltung von Arbeitsanweisungen (SOPs), Packmittel, Management von Reklamationen, Dokumentation von Corrective and Preventive Actions (CAPA), zuverlässiger Austausch von Studiendaten – diese prozessbezogenen, workflowbasierten Lösungen werden – nach der Validierung – auf einer qualifizierten SharePoint-Infrastruktur implementiert. Das Digitale Rechte-Management (DRM) mit entsprechendem Nutzer- und Rollenkonzept und Infrastruktur ermöglicht es, dass auch externe Nutzer auf die Plattform und die Applikationen zugreifen können. So ist eine Orchestrierungsplattform für die an der Wertschöpfungskette beteiligten Partner und Dienstleister verfügbar, die einen regelkonformen Austausch und die gemeinsame Bearbeitung von Daten und Dokumenten ermöglicht. Microsoft SharePoint 2010 und SharePoint 2013 erfüllen die Anforderungen des US FDA 21 CFR Part 11 und des EU GMP Annex 11. ■

Dr. Andreas Jabs,
Principal Consultant
Alegri International Group

Die Informationssicherheit im Unternehmen stärken

Nachhaltiges Risikomanagement ist unverzichtbar

Das Risikomanagement leistet einen wertvollen Beitrag dazu, sich als Unternehmen vor Angriffen, Gefahren und Bedrohungen zu schützen und Schäden zu vermeiden. Zudem ermöglicht es, alle gesetzlichen Vorgaben einzuhalten, und liefert den Nachweis für eine verantwortungsvolle Unternehmensführung.

Auch wenn wir es alle nicht gern hören, Abhörskandale und Datenspionage verdeutlichen uns eindrücklich, dass es mehr Interesse an unseren Informationen gibt, als wir es im Allgemeinen für möglich halten. Dass besonders die Geschäftsgeheimnisse und Werte von technologisch führenden europäischen Unternehmen interessant für andere sind, liegt auf der Hand und wird permanent in zahlreichen Studien zur Cyberkriminalität dokumentiert. Aber auch Datenpannen in Unternehmen oder Organisationen aufgrund mangelnder Kontrolle und lückenhafter Prozesse im IT-Management führen häufig zu hohen, ungeplanten Kosten und Imageverlusten. Doch was ist zu tun? Aufgeben, abwarten und hoffen, dass das eigene Unternehmen nicht betroffen sein wird, oder sinnvolle Schritte unternehmen, um die Risiken zu minimieren? Die Antwort liegt klar auf der Hand.

Risikomanagement als Bestandteil erfolgreicher Unternehmensführung

Heute sind nahezu alle Geschäftsprozesse IT-gestützt und nahezu alle Informationen werden digital be- und verarbeitet. Deshalb leistet operatives Risikomanagement im Bereich Informationssicherheit (IS) einen wesentlichen Beitrag zum erfolgreichen Gesamtrisikomanagement eines Unternehmens oder einer Organisation.

IS-Risikomanagement dient

- dem Schutz vor Gefahren und Bedrohungen,
- der Vermeidung von Schäden und damit
- der Minimierung von Risiken für die Organisation.

Neben der Einhaltung gesetzlicher Vorgaben trägt die Umsetzung eines planvollen, auf die Unternehmensbedürfnisse abgestimmten IS-Risikomanagements wesentlich zum Nachweis verantwortungsvoller Unternehmensführung und der Gewähr der Vertrauenswürdigkeit gegenüber Lieferanten, Kunden, Banken und Versicherungen bei. Wirksames und methodisches IS-Risikomanagement ermöglicht die Verbindung von Geschäftsprozessen, Informationen und IT-Assets. Nur so wird transparent, welche Geschäftsprozesse und Informationen (einschließlich unterstützender Systeme) hochkritisch, kritisch und weniger kritisch sind. Diese Kenntnis erlaubt ein differenziertes Vorgehen und bietet die Möglichkeit,

- auch in einer komplexen IT-Landschaft nachhaltige Prozesse zu etablieren, die Gefahren vorausschauend identifizieren,
- entsprechende Risikobegegnungsmaßnahmen rechtzeitig einzuleiten,
- Kosteneinsparpotenziale bei den Investitionen in technische Produkte, bei den Service-Level-Agreements und durch die Standardisierung von Prozessen zu identifizieren, und
- auf Basis von belegbaren Fakten zu entscheiden und bedarfsgerecht zu agieren.

Wirksames IS-Risikomanagement

Wirksames IS-Risikomanagement muss kontinuierlich betrieben werden, wie es die Plan-Do-Check-Act-Methodik beispielsweise im ISO-Standard 27005 vorsieht. Es sollte in der Lage sein, Geschäftsprozesse und Informationen mit den IT-Assets so zu verbinden, dass alle Geschäftsprozesse und Informationen entsprechend ihrer Kritikalität vollständig, wirtschaftlich und methodisch identifiziert und optimal bedarfsgerecht abgesichert werden können.

IS-Risikomanagement ist zudem dann erfolgreich, wenn es

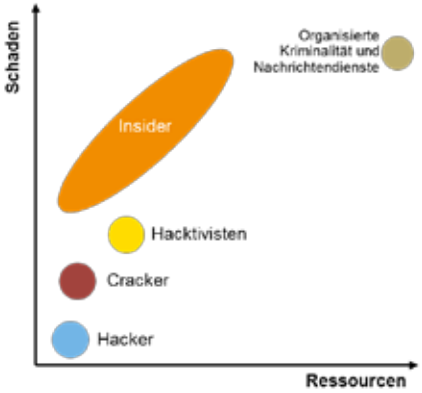
- an den individuellen Erfordernissen des Unternehmens ausgerichtet ist,
- alle branchenspezifischen Anforderungen abbilden kann,
- den Compliance-Anforderungen entspricht und eine vollständige Analyse und Behandlung aller IS-Risiken erlaubt,
- so konzipiert ist, dass es die beteiligten Fachabteilungen dazu motiviert, sich zu beteiligen, auch wenn diese nicht täglich mit der Thematik befasst sind,
- die Verantwortlichen für das IS-Risikomanagement so unterstützt, dass die Kapazitäten für die Kernaufgaben genutzt werden können,
- keine Insellösung ist, sondern die Möglichkeit bietet, die erhobenen Daten über das gesamte Unternehmen bei Bedarf zu aggregieren und zu vergleichen,
- sich soweit möglich in die vorhandene IT-Landschaft integriert, sodass Daten nicht doppelt erfasst werden müssen und über Schnittstellen an andere Systeme, beispielsweise das Gesamtrisikomanagement, übergeben werden können.

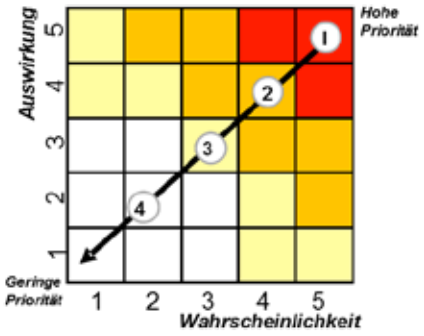
Auf professionelle und erprobte Lösungen vertrauen

Grundsätzlich kann IS-Risikomanagement mit Hilfe von Standard-Software wie beispielsweise Microsoft Excel betrieben werden. Führt man sich jedoch die komplexen

Geschäftsprozesse größerer Organisationen und die damit verbundenen hochintegrierten IT-Landschaften vor Augen, wird schnell deutlich, dass dies ein komplexes Unterfangen ist. Ohne tiefe Kenntnisse bezüglich der erforderlichen Methodik und Umsetzung bzw. der Erfordernisse an ein entsprechendes Datenmodell kommt man schnell vom Weg ab, stößt an technische Grenzen und/oder riskiert am Ende eine teure und nicht den Erwartungen entsprechende Eigenentwicklung.

Ein erfolgversprechender und wirtschaftlicher Weg ist es, auf professionelle und erprobte IS-Risikomanagement-Lösungen zu vertrauen, die häufig auch den Mehrwert eines kompletten IS GRC (Governance, Risk & Compliance) Systems bieten und die Compliance-Anforderungen bereits integrieren. Moderne, benutzerfreundliche Lösungen bringen nicht nur die gesamte Methodik und die Inhalte internationaler Standards (einschließlich bereits umgesetzter Fragenkataloge und Best-Practice-Maßnahmenvorschläge) mit. Systeme, die sich flexibel an die Anforderungen der Anwender anpassen lassen, unterstützen Verantwortliche darüber hinaus durch die Integration und automatische Verknüpfung aller zusammengehörenden Abläufe. Umfassende Berechtigungssysteme moderner Applikationen ermöglichen es auch großen Unternehmen, ihre Strukturen wirtschaftlich in einer Lösung abzubilden. Die Ergebnisse einzelner Organisationen können so verglichen und konsolidiert werden. Lösungsunterstützung im IS-Risikomanagement ermöglicht es, nachhaltig wirtschaftlich und kostengünstig zu arbeiten.





Eine gute Entscheidungshilfe bietet das Qualitätssiegel „IT Security made in Germany", das vom „TeleTrusT Bundesverband IT-Sicherheit e. V." vergeben wird. Lösungshersteller mit diesem Kennzeichen verpflichten sich in besonderem Maße dazu, bei der Herstellung ihrer Produkte strenge Maßstäbe in Bezug auf Sicherheitsanforderungen zu beachten. ■

Ellen Wüpper, Geschäftsführung WMC GmbH

Governance, Risikomanagement und Compliance intelligent verbinden

Informationsschutz mit Methode

Compliance, Governance und Risikomanagement – für alles gibt es Normen und Gesetze. Doch daraus die richtigen Handlungen abzuleiten, ist schwer. Eine methodische und gleichzeitig praxisnahe Herangehensweise ermöglicht es, Schritt für Schritt eine effektive Lösung für den Informationsschutz aufzusetzen.

Die Informationstechnik bildet in Unternehmen wie auch Behörden die Basis für einen optimalen Informationsfluss und effiziente Geschäftsprozesse. Um die Risiken, die der IT-Einsatz mit sich bringt, transparent zu machen und ein angemessenes Sicherheitsniveau zu erreichen, ist ein professionelles Management notwendig. Unternehmen sollten sich dabei an Standards orientieren.

Aufwendungen und Kosten abschätzen

Alle Maßnahmen für den Informationsschutz sind zunächst unter betriebswirtschaftlichen Aspekten zu betrachten. In diese Kalkulation sollten auch die Kosten einfließen, die anfallen, wenn die Richtlinien nicht eingehalten werden. Hierzu zählen beispielsweise die Ausfallzeiten, der Imageverlust und Aufwendungen im Falle von rechtlichen oder strafrechtlichen Maßnahmen. Diese Kosten müssen zu den Aufwendungen für die Umsetzung eines IT-Compliance- und -Security-Konzepts ins Verhältnis gesetzt werden. Unternehmen sollten deshalb methodisch vorgehen und geeignete Maßnahmen Schritt für Schritt entwickeln und aufsetzen. Damit können sie – mit vertretbarem Aufwand – auch künftigen Compliance-Anforderungen nachkommen. Am Ende des Prozesses sollte ein hoch automatisiertes System stehen, das die Basis für alle regulatorischen Maßnahmen bildet.

Governance, Risikomanagement und Compliance

Das Management des Informationsschutzes umfasst die drei Grundpfeiler Governance, Risikomanagement und Compliance. Governance ist die Steuerung der IT unter dem Gesichtspunkt des Schutzes von Daten. Das Risikomanagement liefert die Antworten auf folgende Fragen: Welche Werte sind mit welcher Priorität zu schützen? Welches sind die Schwachstellen? Welche Maßnahmen sollen ausgewählt und umgesetzt werden, um diese Schwachstellen zu beseitigen? Compliance sorgt dafür, dass in allen Geschäftsprozessen sowie im Umgang mit den Daten die gesetzlichen und internen Vorgaben eingehalten werden.

Soll der Informationsschutz einwandfrei funktionieren, sind zunächst Basisrichtlinien zu definieren, die den sicheren Betrieb und den sicheren Umgang mit Daten beschreiben. Diese Richtlinien regeln auch im täglichen Betrieb den Umgang mit Projekten. Grundlegend gilt immer, die Sicherheit und den Informationsschutz kontinuierlich zu verbessern. Formal wird dies durch den Regelkreislauf des Plan-Check-Do-Act sichergestellt.

Methodischer Ansatz für einen effizienten IT-Betrieb unter Sicherheits- und Compliance-Aspekten

Rechte-Analyse

Audit Informationssicherheit

Risiken in gewachsenen Dateisystemen

- erfassen (Scan)
- darstellen (Report)
- bewerten (Analyse)

Migration

Saubere Dateisystem- und Rechtestrukturen

Migration in eine sicher verwaltbare Zielstruktur

- Einfache und einheitliche Dateisystem- und Berechtigungsstrukturen
- Transparenz für regulatorische Anforderungen
- Voraussetzung für die automatisierte Verwaltung

Fileservice-Management

Sichere Verwaltung von Informationen & Rechten

Automatisierte, regelbasierte Verwaltung der Dateisysteme und Berechtigungen

- Prozesse bei Bereitstellung und Verrechtung von Fileservices sind gesichert und durchgängig automatisiert
- Regelverstöße bei der Rechtevergabe werden erkannt
- Sicheres De-Provisioning
- Revisionssichere Dokumentation aller Prozessschritte

IAM & ITSM

Effizienter IT-Betrieb unter Sicherheitsaspekten

Automatisierte Verwaltung von Identitäten, Rechten, Ressourcen und Services

- Verwaltung digitaler Identitäten und Kennungen
- Flexible Prozessgestaltung für User-, File-, Mail-, Voice- und Application-Services
- Einfache und schnelle Prozessänderungen durch Regel-Management
- Self-Service-Funktionen mit Genehmigungs-Workflows
- Rollen- und mandantenbasierende Rechtekonzepte

Mangelhafte Umsetzung

Nahezu jedes Unternehmen und jede Behörde versuchen heute, sich umfassend vor Bedrohungen zu schützen und ein akzeptables Sicherheitsniveau zu erreichen. Oftmals ermitteln sie jedoch nicht, welchen Bedrohungen sie konkret ausgesetzt sind und welche Gegenmaßnahmen sie einleiten sollten. Aber auch der umgekehrte Fall tritt häufig auf: Die ergriffenen Maßnahmen sind nicht wirklich notwendig und die Unternehmen investieren das Geld an der falschen Stelle.

Schritt für Schritt zu mehr Sicherheit

Im ersten Schritt ist es wichtig, dass Unternehmen ihre Ziele klar definieren und folgende Fragen klären: Ist ein technisches Basisniveau ausreichend? Sollen Prozesse eingeführt und umgesetzt werden, die dafür sorgen, dass das Sicherheits- und Compliance-Niveau weitgehend automatisiert kontinuierlich ansteigt? Sollen Richtlinien erstellt werden, um die IT daran zu messen? In jedem Fall sollte das Hauptziel sein, Transparenz zu schaffen und zu erkennen, welche Mängel es in der IT-Infrastruktur zu beseitigen gibt und wie diese zu beseitigen sind. Im Zuge dieser Analyse finden sich oftmals viele Anhaltspunkte, wie Unternehmen ihren IT-Betrieb optimieren und gleichzeitig die Kosten senken können. IT-Security-Workshops ermöglichen es, diese Themen praxisnah zu bearbeiten und in einer offenen Diskussion über die bestehende IT-Landschaft und oftmals eingefahrene Prozesse zu sprechen.

Optimale Vorgehensweise

Planung und Einführung eines Managementsystems für Informationsschutz

- Aufbau einer Policy-Struktur
- Erstellung von Policies (Allgemeine Leitlinien und Sicherheitsrichtlinien)
- Planung und Aufbau einer Sicherheitsorganisation
- Trainings- und Awareness-Maßnahmen

Unterstützung des IT-Risikomanagements

- Erarbeitung einer Methodik, wie IT-Risiken zu behandeln sind
- Beschreibung der Schnittstellen zum Risikomanagement
- Schutzbedarfsermittlung
- Bedrohungs- und Risikoanalyse
- Ermittlung der Risiken und Definition der geeigneten Maßnahmen
- Bewertung von Risiken
- technische Analyse der Infrastruktur
- Einsatz von unterstützenden Tools

Vorbereitung zur Zertifizierung nach ISO 27001

Folgendes Vorgehen hat sich in der Praxis bewährt:

- Ist-Analyse im Gespräch mit Toolunterstützung (wie beispielsweise Matrix Studio von econet oder Enterprise Security Reporter von ScriptLogic)
- Ausarbeitung eventueller Defizite und Dokumentation
- Abstimmung der Prioritäten
- Klärung der weiteren Vorgehensweise

Den passenden Partner finden

Ein komplexes und heterogenes Umfeld erfordert vielschichtige und individuelle Lösungen. IT-Verantwortliche sollten sich deshalb an Spezialisten wenden, um ihre Projekte für den Informationsschutz umzusetzen. Unternehmen sollten bei der Auswahl des Dienstleistungspartners darauf achten, dass die mitwirkenden Personen auf langjährige Praxis zurückgreifen können und ihr Wissen auch verständlich kommunizieren können. Der Erfolg des Projekts wird letztlich immer daran gemessen, ob die selbst auferlegten Ziele nicht nur erreicht, sondern auch dauerhaft gehalten, wenn nicht verbessert werden können. ■

Dr. Markus Morawietz,
Managing Partner
Dr. MORAWIETZ
Consulting & Training GmbH

IT-Compliance &
IT-Governance

Die Informationssicherheit im Unternehmen stärken

Maßgeschneiderte Lizenzierung schafft Einsparpotenziale

Migration, Virtualisierung, Cloud Computing, Software as a Service (SaaS) – das sind die aktuellen Trends in der IT-Branche. Unternehmen versprechen sich von diesen neuen Lösungen und Leistungsangeboten vor allem Einsparpotenziale. Allerdings gibt es auf dem Weg dahin einige Klippen zu umschiffen – vor allem im Bereich der Lizenzierung.

Viele Unternehmen setzen zunehmend auf Virtualisierungstechnologie, vor allem, wenn sie damit die Performance ihrer IT-Infrastruktur steigern und ihre Kosten senken können. Bei der Lizenzierung von Software in virtuellen Umgebungen gelten jedoch teils andere Regelungen. Den Verantwortlichen und Entscheidern in den Unternehmen ist dies oftmals nicht bewusst, und somit können sie auch keine fundierten Entscheidungen für das Unternehmen treffen.

Planung ist das A und O

Der Erwerb eines Wirtschaftsguts setzt voraus, dessen Einsatz richtig zu erfassen, zu planen und umzusetzen. Zwar ist der Preis durchaus ein wichtiges Kriterium, aber fehlgeplante Investitionen durch „Geiz-ist-Geil"-Mentalität sind unter Umständen extrem kostspielig. Nur weil ein ähnliches Produkt ähnliches kann und kostengünstiger ist, heißt es noch lange nicht, dass es auch das richtige ist. Noch gravierender wirkt es sich aus, wenn das Produkt in seinen Funktionen und Nutzungsrechten nicht umfassend bewertet werden kann. Mit den Worten „Ein Office ist ein Office" ist wohl der größte aller Fehler genannt. Denn seit Langem sind bei Software nicht mehr die Bits & Bytes maßgebend für eine Lizenzierung, sondern viel mehr die Nutzung des Programms. Die Nutzung einer Software ist die Grundlage für die richtige Lizenzierung, also auch die Grundlage für eine sinnvolle Investition. Fragt man einen IT-Leiter, wer für die korrekte Lizenzierung im Unternehmen verantwortlich ist, erhält man sehr oft

als Antwort: „der Geschäftsführer". Fragt man hingegen den Geschäftsführer, lautet in vielen Fällen die Antwort: „der Administrator" oder auch „mein Dienstleister". In allen Antworten steckt Wahrheit. Viel wichtiger als die Zuweisung der Verantwortlichkeit aber ist es, die IT-Struktur so zu planen, dass sich diese Fragen gar nicht erst stellen. Eine dieser Grundlagen ist Software Asset Management, die Einführung von Prozessen, die den Softwarebestand eines Unternehmens verwalten, kontrollieren und schützen können.

Transparenz schaffen

Viele Entscheidungen im Umfeld von Softwarebeschaffung basieren auf Halbwissen und Schätzung: Halbwissen darüber, wie die Lizenzen eingesetzt und genutzt werden dürfen. Schätzung des tatsächlichen Bedarfs, der Anzahl von nutzenden Mitarbeitern und Geräten. Diese Zahlen stellen dann die Bewertungsgrundlage für Investitionen dar und werden in der Regel nicht exakt erhoben – geschweige denn aktualisiert. Dies kann zu einer fehlerhaften Lizenzplanung und damit zu einer fehlerhaften Lizenzierung führen. „Entscheider sollten eine dauerhafte und wirtschaftliche Lösung für die Softwarenutzung finden. Dazu benötigen sie fundiertes Lizenzwissen, belastbare Zahlen, einen kontinuierlichen Überprüfungsprozess und Regeln für den Umgang mit Software. Nur das schafft Transparenz", erklärt Carsten Donath, Geschäftsführer bei der SFC Software for Companies GmbH.

Die Lösung heißt Software Asset Management

Lizenzierung ist ein komplexes Thema. Es kann aber nicht das Ziel sein, aufgrund dieser Komplexität eine dauerhaft fehlerhafte Lizenzierung zu akzeptieren. Die erforderliche Transparenz erhalten Unternehmen durch Software Asset Management (SAM). SAM gibt den Verantwortlichen Aufschluss darüber, welche Anwendungen grundsätzlich im Unternehmen vorhanden sind, wie diese verwendet werden und welche Lizenzarten und -modelle diesen Anwendungen zugrunde liegen. Zudem unterstützt Software Asset Management Unternehmen dabei, klare Prozesse für die Anschaffung, den Einsatz und die Nutzung der Software zu definieren und umzusetzen. Aktives Software Asset Management bildet die Basis für fundierte Entscheidungen in der Softwarebeschaffung und ermöglicht es, Fehlentscheidungen zu vermeiden. Mit einer zielgerichteten und klaren Planung sowie einer durchdachten Strategie können Unternehmen ihre Kosten senken und ihre künftigen Aufwendungen und finanziellen Investitionen genau einschätzen. ■

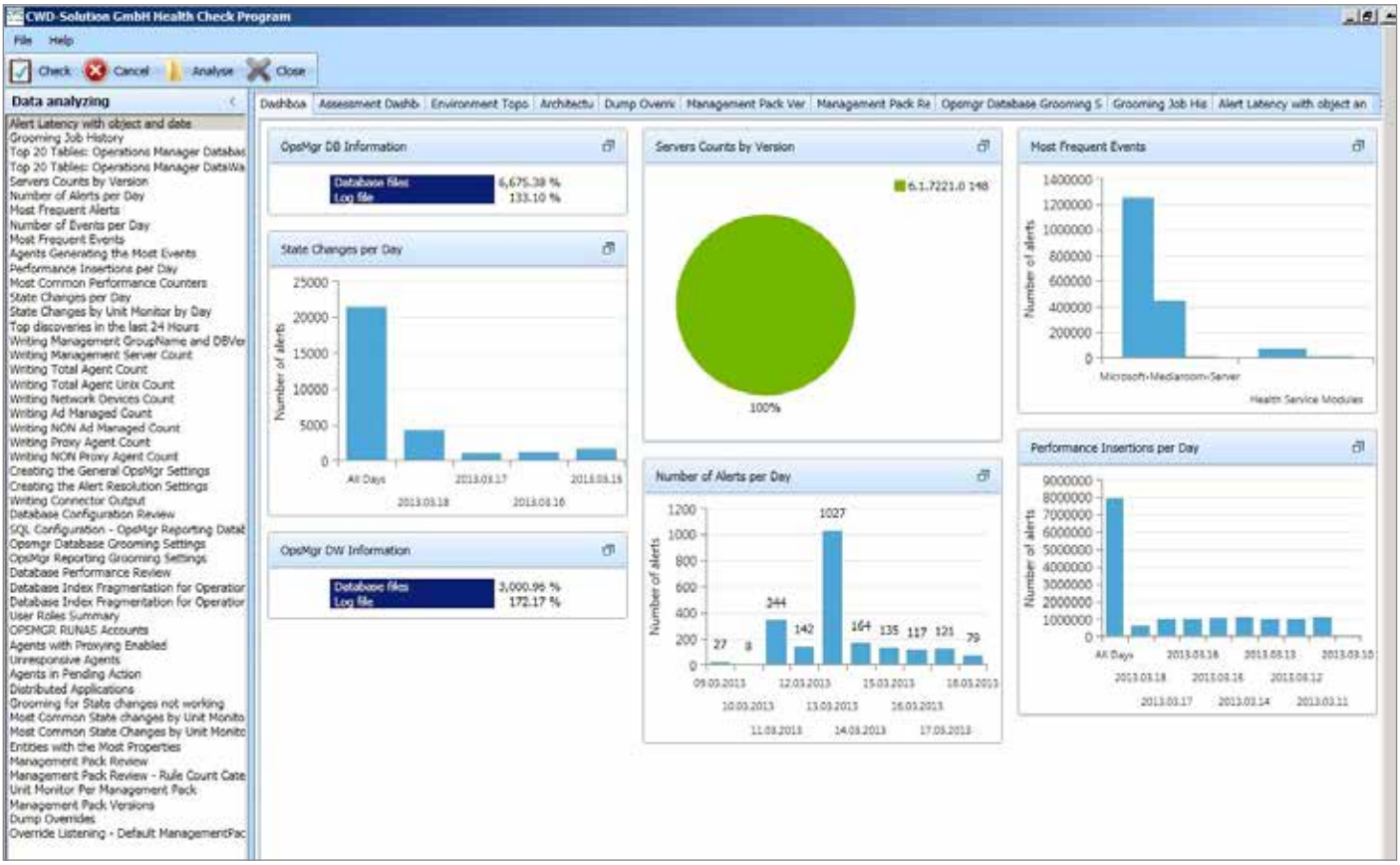
Carsten Donath,
Geschäftsführer
SFC Software for Companies GmbH

Produkte & Technologien

Optimal geschützt vor rechtlichen Sanktionen

Auf der sicheren Seite

IT-Compliance stellt für viele Unternehmen eine große Herausforderung dar – sei es für das Management oder für die IT-Verantwortlichen und Administratoren. Die Microsoft System Center Suite und das Health Check Analyzing Program der CWD-Solution GmbH unterstützen Unternehmen optimal dabei, sich einen detaillierten Überblick über die IT-Infrastruktur zu verschaffen und Probleme zu identifizieren und zu beheben.



Das Health-Check-Dashboard der CWD-Solution GmbH

Unter dem Begriff „Compliance" ist allgemein die Einhaltung von Regeln zu verstehen. Hierzu zählen beispielsweise Gesetze, Richtlinien, vertragliche Verpflichtungen oder auch unternehmensinterne Regeln und Vorgaben. Daneben steht der Begriff für freiwillige Kodizes in Unternehmen. Dieser zielt auf eine vorgelebte Unternehmensethik ab, die nicht zu unterschätzende, positive Auswirkungen auf die Effizienz von Geschäftsprozessen sowie die Kosten- und Ertragsstruktur eines Unternehmens hat.

IT-Compliance – regelkonform agieren

Diese Aspekte müssen im heutigen IT-Umfeld genauso beachtet werden wie systemrelevante Anforderungen an Hard- und Software. IT-Compliance will die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und Mitarbeiter des Unternehmens sowie gegebenenfalls von Dritten, um teils empfindliche, existenzgefährdende, rechtliche Sanktionen abzuwenden. Dies umfasst auch die Bereiche Datenschutz, Datenaufbewahrung, Verfügbarkeit und Informationssicherheit. Um diesen Anforderungen gerecht zu werden, hat Microsoft mit der System Center Suite ein mächtiges Werkzeug geschaffen, mit dem Unternehmen ihre IT-Infrastruktur optimal verwalten und ihre Prozesse anpassen und automatisieren können. Proaktives Monitoring sorgt für die nötige Ausfallsicherheit, und umfangreiche Reporting- und Backup-Funktionen stellen Nachhaltigkeit sicher. Und dies ist nur ein kleiner Auszug aus dem Leistungsspektrum der einzelnen Produkte, die die System Center Suite bietet.

Risiken minimieren

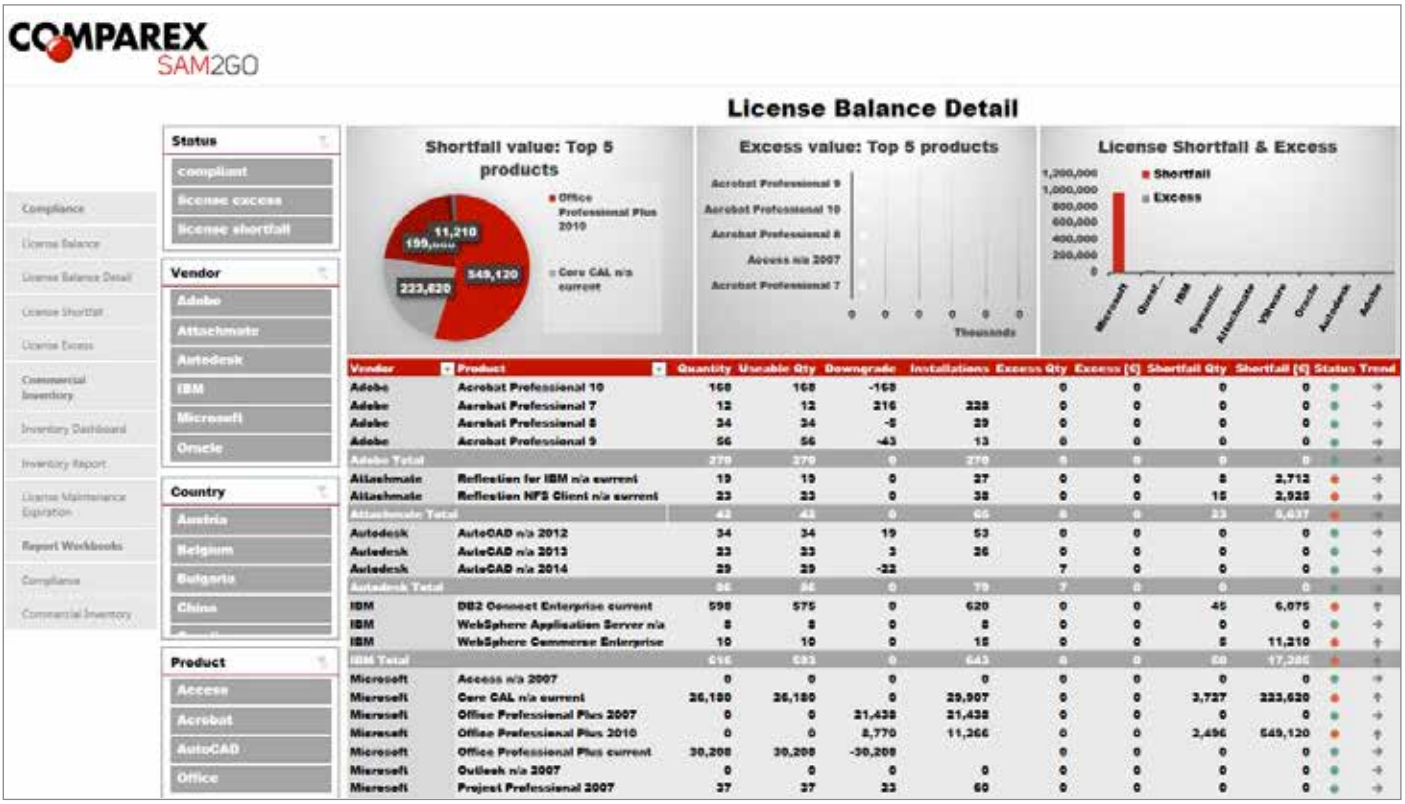
Doch trotz des großen Umfangs der Microsoft System Center Suite und jahrelanger Erfahrung bei der Verwaltung und Überwachung von kleinen und großen IT-Strukturen und stetiger Weiterentwicklung – ein Restrisiko bleibt. Durch fehlerhafte Planung, falsche Konfigurationen oder Bedienfehler können Sicherheitslücken entstehen, die meist erst viel zu spät oder gar nicht entdeckt werden. Hier setzt die CWD-Solution GmbH mit ihren Health-Checks an. Diese Lösung basiert auf der jahrelangen Erfahrung und dem fundierten Praxis-Know-how aus den unterschiedlichsten Projekten und Umgebungen. Health-Check der CWD-Solution GmbH unterstützt Unternehmen dabei, aktiv Probleme zu identifizieren und Fehlstände in der IT-Infrastruktur aufzudecken und zu beheben. Darüber hinaus bieten die erfahrenen und kompetenten Berater der CWD-Solution GmbH Unterstützung an und führen Health-Checks in Unternehmen durch – von der Auswertung und Analyse der Ist-Situation bis hin zur Fehlerbehebung. ■

Matthias Schmitz,
Berater der
CWD-Solution GmbH

Planungs- und Rechtssicherheit erhöhen, Kosten senken

Software Asset Management – Pflicht oder Kür?

Nutzt ein Unternehmen mehr Software als lizenziert, kann es richtig teuer werden. Unwirtschaftlich ist es jedoch, wenn erworbene Lizenzen brachliegen. Ein professionelles Software Asset Management (SAM) zahlt sich daher schnell aus. Neben optimierten Kosten sorgt es für klare Fakten bei strategischen Software-Entscheidungen und Compliance-Fragen.



Mit SAM2GO ist die Lizenzbilanz auf Knopfdruck jederzeit verfügbar.

Welche Software wird in welcher Abteilung wie häufig genutzt? Sind die Programme über- oder unterlizenziert und mit welcher Summe schlagen sie tatsächlich zu Buche? Diese Fragen lassen sich in vielen Unternehmen nicht eindeutig beantworten. Dabei kann der wirtschaftliche Schaden einer unübersichtlichen Softwareverwaltung beträchtlich sein. Hinzu kommt die rechtliche Unsicherheit, denn selbst mit unwissentlich falsch genutzter Software verletzten die Anwender das Urheberrecht.

Verlässliche Antworten hingegen liefert ein professionelles Software Asset Management (SAM). Es umfasst alle Maßnahmen zur Beschaffung, Verteilung, Nutzung und Wartung von Software. Es geht darum, die Nutzung von Software transparent und effizient zu organisieren sowie den Softwarebestand über seinen gesamten Lebenszyklus zu kontrollieren und kontinuierlich auf dem neuesten Stand zu halten.

Lizenzmanagement schafft Transparenz

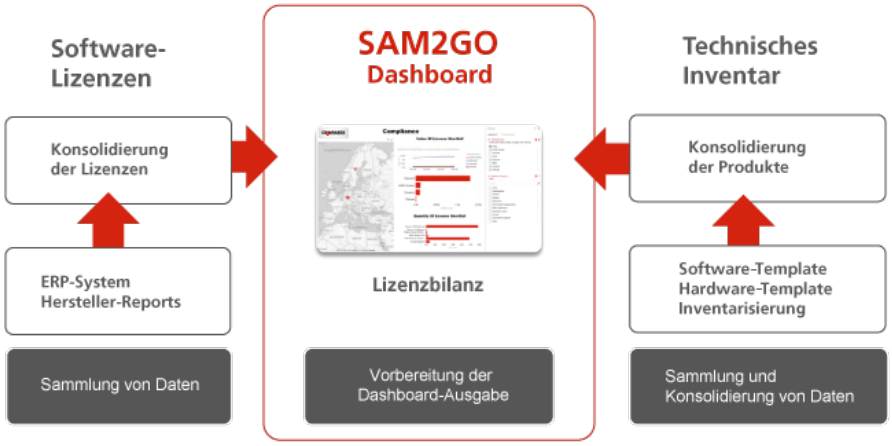
Je komplexer eine Umgebung wird, desto notwendiger wird Transparenz. So kann beispielsweise die Einführung neuer Hardware schnell zu einer Unterlizenzierung führen, wenn diese mehr Prozessoren hat als die alte. Auch lässt sich die Kostenfrage vor dem Rollout einer neuen Software oder der Einführung eines neuen Betriebssystems nur klären, wenn der aktuelle Lizenzbestand klar und seine Nutzung transparent ist.

Ein professionelles SAM verschafft nicht nur den erforderlichen Überblick, sondern liefert auch die Basis für die Einführung neuer strategischer Konzepte wie etwa BYOD. Es

bringt zahlreiche Informationen auf den Tisch, die den Ansatz für neue Lösungen beinhalten respektive deren Einführung erleichtern. Dazu gehören verlässliche Kennzahlen zu IT-Infrastruktur, IT-Kosten, eingesetzter Software sowie Hardware. Ziel ist es, mittel- bis langfristige Kosteneinsparungen zu realisieren.

SAM im Praxiseinsatz

Doch wie findet ein Unternehmen genau das SAM-Werkzeug, das sich für seine individuellen Anforderungen eignet? Rödl & Partner, eine Beratungs- und Prüfungsgesellschaft für die Gebiete Wirtschaft, Steuern, Recht und IT, haben sich dafür Experten ins Haus geholt. Um im Anschluss an ein unternehmensweites Compliance-Projekt nachhaltig die gewonnene Transparenz zu erhalten, fiel die Entscheidung auf die Lösung SAM2GO von Comparex. Im ersten Schritt wurden der Software-Bedarf ermittelt und die Lizenzierung optimiert. Im Sinne eines nachhaltigen Lizenzmanagements wird diese Bilanz als Managed Service im vierteljährlichen Turnus weiter gepflegt und bei Bedarf um die Software weiterer Hersteller erweitert. Der Vorteil für Rödl & Partner: Sie können nun mit niedrigeren Kosten für ihr Software Asset Management kalkulieren, da keine Investitionen in Hardware, Tools oder Maintenance nötig sind. Auch der organisatorische Aufwand verringert sich für das Unternehmen und seine Mitarbeiter deutlich. Hinzu kommt das Plus an Sicherheit, denn im Falle einer Prüfung durch einen Softwarehersteller ist das Unternehmen jederzeit auskunftsfähig. ■



Christian Terwiel,
International Product Manager SAM
COMPAREX AG

Gefahren gezielt minimieren

E-Mail-Kommunikation ohne Risiko

Mit der intensiven Nutzung von E-Mails als wichtigstem Medium in der geschäftlichen Kommunikation steigen auch die Gefahren. Gezielte Spam-Abwehr, umfassender Schutz vor Schadsoftware und eine lückenlose Ende-zu-Ende-Verschlüsselung gewährleisten, dass Unternehmen auch weiterhin auf E-Mails in ihrer Kommunikation vertrauen können.

Täglich milliardenfach verschickt, halten E-Mails weltweit private und geschäftliche Beziehungen am Laufen – schnell, einfach und effizient. Aber nicht unbedingt sicher: Den Löwenanteil des Posteingangs machen nach wie vor Spam und mit Malware infizierte Nachrichten aus. Auch der vermeintlich sicheren Business-Kommunikation droht Gefahr. Der PRISM-Skandal hat gezeigt, wie riskant es ist, Geschäftsdaten unverschlüsselt und für die ganze Welt einsehbar zu verschicken. Unternehmen, die E-Mails weiterhin als produktiven Teil ihrer Business-Kommunikation nutzen möchten, sind auf starke E-Mail-Sicherheit angewiesen. Eine tragfähige Sicherheitsarchitektur muss dabei auf drei wichtigen Säulen aufbauen:

- lückenloser Ende-zu-Ende-Verschlüsselung
- effizienter Spam-Abwehr
- zuverlässigem Malware-Schutz

Lückenlose Ende-zu-Ende-Verschlüsselung

Starke E-Mail-Verschlüsselung ist für Business-Umgebungen unverzichtbar. Als Hersteller und Integrator hat Net at Work die Erfahrung gemacht, dass sich Verschlüsselung am besten auf einem zentralen Gateway implementieren lässt. Anwender haben somit kaum Berührungspunkte mit der Technologie. Das von Net at Work entwickelte Gateway enQsig nutzt für die Verschlüsselung wahlweise S/MIME, PGP-Schlüssel oder PDF-Mail und verfügt zudem über einen providerunabhängigen, zertifizierten De-Mail-Konnektor für einen sicheren, zentralen Zugang zum De-Mail-System. Dabei ist enQsig für eine nahtlose Integration in

Microsoft-Umgebungen optimiert. So unterstützt das Mail-Gateway beispielsweise die Zertifikate interner Active-Directory-Zertifizierungsstellen, um eine schnelle und günstige Umsetzung von Verschlüsselungsprojekten zu ermöglichen. Die Verteilung der Zertifikate kann über die Gruppenrichtlinien des Active Directory ebenfalls äußerst effizient gesteuert werden. Am Arbeitsplatz lässt sich enQsig über ein Software-Add-In nahtlos in bestehende Microsoft Outlook-Umgebungen einbinden. Das Add-In erweitert die Outlook-Leiste um intuitiv verständliche Symbole, mit denen Anwender ihre E-Mails auf Knopfdruck verschlüsseln und signieren können.

Effiziente Spam-Abwehr

Der Spam-Anteil an der E-Mail-Kommunikation ist ungebrochen hoch. Die Experten des israelischen Security-Herstellers Commtouch beziffern ihn aktuell auf 74 bis 78 Prozent. Ein starker Spam-Filter ist für Unternehmen damit nach wie vor eine absolute Notwendigkeit. Die meisten klassischen Spam-Filter erreichen bei der Abwehr solide Trefferraten, haben aber immer noch mit dem Problem der „False Positives" zu kämpfen: Stellt man den Filter so restriktiv ein, dass er Spam zuverlässig blockt, werden automatisch auch relevante Nachrichten ausgesiebt. Der Schaden durch die falsch klassifizierten E-Mails ist erheblich und unmittelbar, da der Absender nicht erfährt, dass seine Nachricht nicht angekommen ist. Das von Net at Work entwickelte Anti-Spam-Gateway NoSpamProxy ist zwar auch nicht gänzlich gegen False Positives gefeit – aber im Gegensatz zu anderen Lösungen nimmt NoSpamProxy die Spam-E-Mails gar nicht erst an. Die Lösung analysiert Spam-E-Mails schon während der Übertragung mit einer Reihe von Text- und Reputationsfiltern und bricht den Transfer gegebenenfalls ohne Annahme ab. Der Absender erhält von seinem eigenen E-Mail-Server eine Unzustellbarkeitsnachricht über die gescheiterte Zustellung. Wurde er zu Unrecht geblockt, weiß er, dass seine Nachricht nicht zugestellt wurde, und kann über einen anderen Weg den Kontakt suchen. Um sicherzustellen, dass relevante Kommunikationspartner nicht geblockt werden, nutzt NoSpamProxy zusätzlich einen individuellen „Level-of-Trust"-Filter, der bei jeder ausgehenden E-Mail automatisch Vertrauenspunkte für

den Empfänger hinterlegt. Schickt dieser seinerseits eine E-Mail zurück, ist deren Zustellung aufgrund des hinterlegten Vertrauensbonus garantiert – auch dann, wenn die übrigen Spam-Filter eigentlich zu einer Ablehnung führen würden. Mit Viren infizierte E-Mails werden trotz Vertrauenspunkten weiterhin geblockt.

Zuverlässiger Schutz vor Malware

Viren, Würmer und Trojaner richten jedes Jahr verheerende Schäden an. Bei der Verbreitung der Schadsoftware kommt der E-Mail nach wie vor eine Schlüsselrolle zu: Mal steckt die Malware ganz klassisch in angehängten Dateien, mal verbirgt sie sich hinter Links im Inhalt oder in kompromittierten PDFs. NoSpamProxy verwendet eine Reihe leistungsfähiger Filtertechnologien, um das Eindringen von Malware zuverlässig zu verhindern. Einer der wirkungsvollsten davon ist die „Zero-Hour Virus Protection" von Commtouch. Der Echtzeitfilter basiert auf der Recurrent Pattern Detection (RPD) – einer content- und sprachunabhängigen Analyse, die Malware anhand des Verbreitungsmusters stoppt, bevor sie das Netzwerk erreicht. Das Verfahren funktioniert äußerst zuverlässig und zeichnet sich vor allem durch minimale False-Positive-Quoten aus. Da RPD nicht patternbasierend arbeitet, bietet Commtouch zudem bereits während der Zero-Day-Phase eines Virenausbruchs, sprich vor dem Erscheinen der aktuellen Pattern-Files, zuverlässigen Schutz. Ergänzend dazu unterstützt NoSpamProxy eine Reihe weiterer Filter, darunter auch eine signaturbasierende Komponente, wie sie von klassischen Antiviren-Produkten bekannt sind.

Implementierung als zentrales Security-Gateway

Bei der Implementierung einer dreistufigen E-Mail-Security-Architektur stehen Unternehmen eine Vielzahl von Optionen zur Verfügung. Net at Work empfiehlt den Einsatz eines zentral betriebenen Mail-Security-Gateways, das Anti-Spam, Anti-Virus und Verschlüsselung als dedizierte Module bereitstellt. Diese Konstellation garantiert ein hohes Sicherheitsniveau, ist einfach zu verwalten und lässt sich flexibel lizenzieren. ■

Net at Work

Die Net at Work Netzwerksysteme GmbH ist ein seit 1995 bestehendes Software- und Systemhaus mit Sitz in Paderborn (www.netatwork.de). Die beiden Gründer und Gesellschafter des Unternehmens sind der Geschäftsführer Uwe Ulbrich sowie Frank Carius. Net at Work vertreibt die Anti-Spam-Lösung NoSpamProxy sowie die Verschlüsselungslösung enQsig. Als Systemhaus und Mitglied im Microsoft Partner Network mit Gold-Kompetenz bietet Net at Work Unternehmen aus allen Branchen zudem Lösungen zur Optimierung ihrer Geschäftsprozesse.

Frank Carius, Gründer des Unternehmens Net at Work und Betreiber von www.msxfaq.de

Maximale Flexibilität dank Software Defined Archiving

Hardwareunabhängige Datenaufbewahrung schafft langfristige Sicherheit

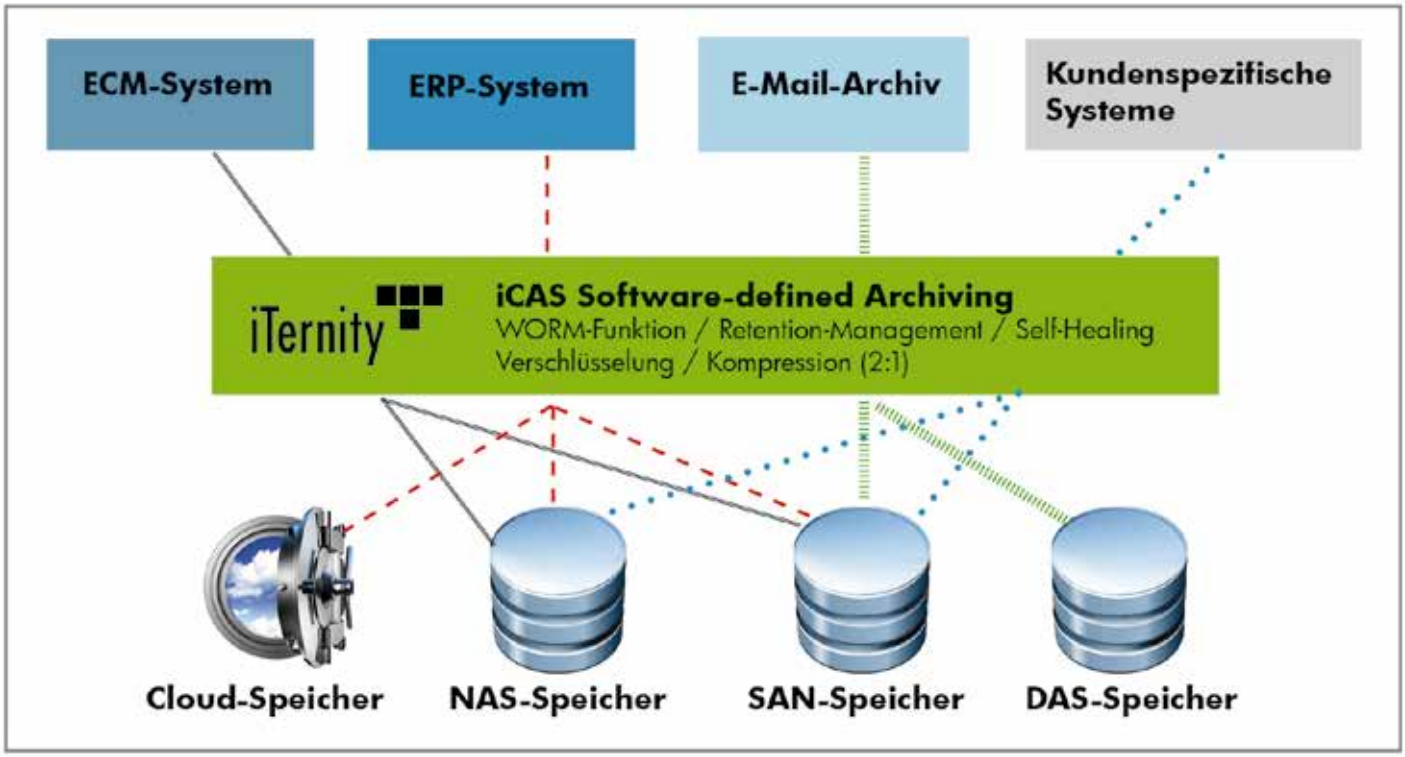
Angesichts der ungebremst wachsenden Menge unstrukturierter Daten sehen sich Unternehmen und Organisationen aller Art mit neuen Anforderungen an das Informationsmanagement konfrontiert. In diesem Zusammenhang spielen steigende Compliance-Anforderungen, zu denen unter anderem die rechtssichere Archivierung und Informationssicherheit gehören, eine immer größere Rolle.

Unternehmen stehen heute vor der Aufgabe, mit optimaler IT-Effizienz die Kosten für die Speicherung und Archivierung ihrer enormen Datenmengen (Big Data) unter Kontrolle zu behalten. Gleichzeitig müssen sie die gesetzlichen Richtlinien und internen Anforderungen an den langfristigen Schutz und die Aufbewahrung der Daten erfüllen. Ziel dabei ist es, die Geschäftsrisiken, die durch einen Datenverlust entstehen können, zu minimieren, und die Beweisfähigkeit der archivierten Daten sicherzustellen.

Lassen sich diese Anforderungen angesichts immer kürzerer Innovationszyklen in der Speicherindustrie noch mit herkömmlichen Speicher-Silos befriedigend erfüllen? Der Software-Hersteller iTernity bietet mit iCAS eine Alternative für genau diese Anforderungen – basierend auf Microsoft-Technologien und Industriestandards. Die iTernity Compliant Archiving Software (iCAS) lässt sich einfach in jegliche IT-Infrastruktur integrieren und unterstützt NAS-und SAN-Speichersysteme verschiedenster Hersteller. Kunden profitieren somit von der Hardwareunabhängigkeit der Lösung sowie der damit entstehenden Flexibilität und Investitionssicherheit.

Zentrale, hochverfügbare und sichere Archivplattform

iCAS schützt und speichert Archivdaten aus verschiedensten Anwendungen revisionssicher auf festplattenbasierten Speichersystemen. Mit der KPMG-zertifizierten Lösung lässt sich somit auch vorhandener Speicher als Archivmedium nutzen. iCAS gewährleistet dabei die Integrität der Daten unter Einhaltung der höchsten Sicherheits- und Compliance-Standards. Da die patentierten iCAS Archiv-Container selbsttragend sind, bleiben die Daten unabhängig vom Speicherort und -medium immer verifizierbar und auditfähig. Die integrierte



"Es ist nicht die stärkste Spezies die überlebt, auch nicht die intelligenteste, es ist diejenige, die sich am ehesten dem Wandel anpassen kann."

Charles Darwin

Datenreplizierung gewährleistet zudem eine sehr hohe Verfügbarkeit des Archivs ohne zusätzliche Spiegeltechnologien. Alle namhaften ECM-, ERP-, PACS- und E-Mail-Archiv-Systeme sind für iCAS zertifiziert. Damit ist sichergestellt, dass iCAS auch bei einem Systemwechsel als zentrale Archivplattform eingesetzt werden kann. iCAS läuft auf Windows Server 2012 und 2008-R2 Systemen und erweitert diese somit um Archivfunktionalitäten.

Zukunftssicherheit garantiert

Aufgrund der langen Aufbewahrungsfristen von zehn, 30 oder mehr Jahren und der rasanten technologischen Weiterentwicklungen im Speicherbereich ist die Anpassungsfähigkeit von Archivlösungen von höchster Bedeutung. Der Ansatz „Software-defined Storage" (SDS) von iCAS ist dafür ideal geeignet: Die kontinuierliche Datenüberprüfung von iCAS stellt die Integrität der Daten langfristig sicher – und das unabhängig von der Speicherhardware. Falls korrupte Daten gefunden werden, können diese mit der Self-Healing-Funktionalität von iCAS automatisch repariert werden. Damit bleiben geschäftskritische Daten nicht nur langfristig verfügbar sondern auch valide.

Für eine langfristige Verfügbarkeit ist es zudem wichtig, dass archivierte Daten möglichst einfach und schnell auf neue Technologien oder Speichersysteme migriert werden können. Auch das gewährleistet iCAS, da spezielle Funktionen eine rechtskonforme Migration mit Protokollierung des Migrationsprozesses und Verifizierung der kopierten Daten ermöglichen.

Daten können optional auch verschlüsselt (AES-256) werden, um höchste Sicherheitsanforderungen (z. B. PCI-DSS) zu erfüllen. Bei der Anbindung von Cloud-Speicherlösungen werden die Daten vor der Übertragung grundsätzlich verschlüsselt, um eine sichere Übertragung und Ablage zu gewährleisten.

Rechtssicherheit unabhängig geprüft

Die Konformität von iCAS mit den gesetzlichen Richtlinien für die ordnungsgemäße Buchführung und die Unveränderbarkeit der archivierten Daten ist gesichert. iCAS wurde diesbezüglich unter anderem durch die Wirtschaftsprüfergesellschaft KPMG begutachtet und zertifiziert. Wählen IT-Verantwortliche eine Archivlösung, die entsprechend zertifiziert und von Wirtschaftsprüfern eingehend geprüft ist, können sie erheblichen Aufwand einsparen.

Storage Compliance für Microsoft-Umgebungen

iTernity iCAS basiert auf der jeweils neuesten Microsoft-Server-Technologie und lässt sich optimal in Microsoft-Systemlandschaften einbinden. Damit profitiert iCAS auch automatisch von den aktuell unterstützten Funktionen und Verbesserungen auf Betriebssystemebene. Zudem lässt sich iCAS als virtualisierte, kosteneffiziente Lösung implementieren, beispielsweise auf Microsoft® Hyper-V™.

Wirtschaftlichkeit zählt

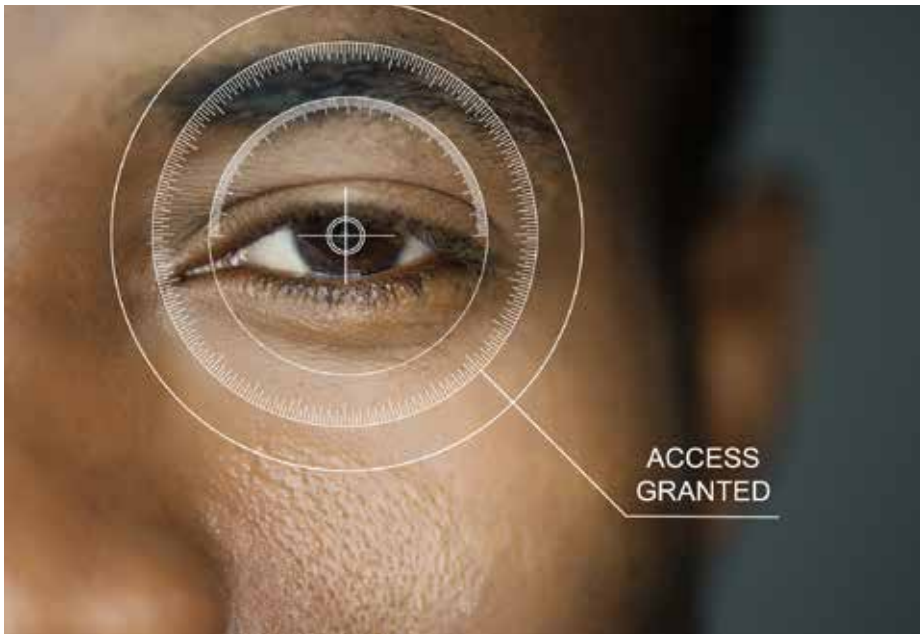
iCAS ermöglicht es, vorhandene Speicherkapazitäten effizient zu nutzen und damit deutliche Kosteneinsparungen zu realisieren, da die Investitionen in Hardware, Software und Personal-Know-how geschützt sind. Da keine gesonderten Storage-Silos für die Archivdaten notwendig sind, entfallen die Anschaffungs- und Betriebskosten hierfür vollständig. Auch die Implementierung von iCAS als Windows-Software oder virtuelle Appliance erfolgt denkbar einfach und reduziert den Implementierungsaufwand enorm. Das transparente Lizenzmodell orientiert sich am Kundenbedarf und basiert auf dem Netto-Archivvolumen oder den genutzten CPUs des iCAS Servers. Bei redundanter Datenspeicherung entstehen also keine Mehrkosten für Lizenzen. Gleichzeitig werden zusätzliche Replizierungslösungen auf Speicherebene überflüssig. ■

Georg Csajkas,
Leiter Product Management und Marketing
iTernity GmbH

Risiken reduzieren, die Produktivität steigern und Compliance erreichen

Modernes Identity Management für mehr Sicherheit und Effizienz

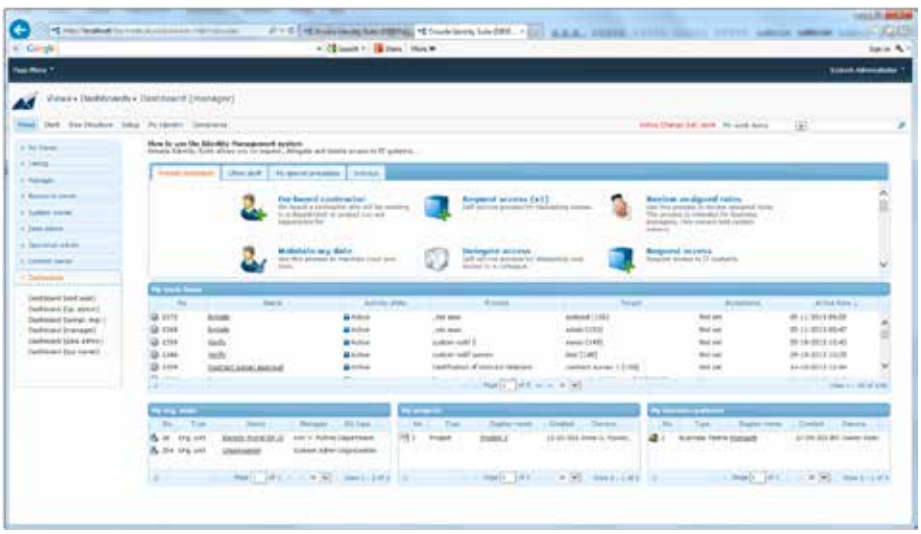
Alle Abteilungen im Unternehmen – von der Geschäftsleitung über die Verwaltung, die Produktion bis zum Außendienst – sind dem Risiko ausgesetzt, dass sensible Unternehmensdaten verloren gehen oder gestohlen werden. Eine der wichtigsten präventiven Maßnahmen ist die Einführung einer Identity-Management-Lösung.



Ziel einer umfassenden Lösung für das Identity Management ist es, eine effiziente Berechtigungsverwaltung sowie Kontrollverfahren für das Risikomanagement zu implementieren. Damit lassen sich Risiken aufdecken, automatisiert beseitigen und bereits während der Rechtevergabe vermeiden. Dabei ist es wichtig, die Fachabteilungen mit einzubeziehen, die Sensibilität für die Notwendigkeit einer effektiven Benutzerverwaltung zu schaffen und die Kollegen aktiv in die Definition der Prozesse und deren Umsetzung einzubinden. Nur wenn der Mehrwert eines Identity Managements für die Fachabteilungen im Unternehmen zu erkennen ist, wird ein System für die Benutzerverwaltung auch aktiv genutzt, und die implementierten Kontrollmechanismen und Regeln können wirksam werden. Wenn Mitarbeiter neue Berechtigungen über ein Self-Service-Portal mit Warenkorb beantragen, ihre Rollen definieren oder persönliche Daten wie Raumnummer, Mobiltelefonnummer und Titel eigenständig pflegen können, werden auch die IT-Abteilungen in den Unternehmen von diesen Routinearbeiten entlastet.

Steigenden Anforderungen gewachsen sein

Aussagekräftige Reports und Funktionen für die Rezertifizierung unterstützen Fachabteilungen dabei, den Status der Berechtigungen kontinuierlich und effizient zu prüfen und die steigenden Compliance-Anforderungen zu bewältigen. Eine regelmäßige Prüfung aller vergebenen Rechte einmal pro Jahr und für privilegierte Berechtigungen alle sechs Monate, wie unter anderem von MaRisk für Banken vorgegeben, ist mit dem Versand von Listen nicht effektiv und sicher umzusetzen. Eine Identity-Management-Lösung muss es ermöglichen, die zu prüfenden Rechte den verantwortlichen Mitarbeitern übersichtlich und leicht verständlich als Entscheidungsgrundlage zusammenzustellen. Zudem



Übersicht für die Fachabteilung: alle relevanten Informationen auf einen Blick

Skalierbare Benutzerverwaltung

Das dänische Unternehmen Omada bietet eine flexible und skalierbare Lösung für das Identity Management an, die sowohl die Automatisierung der Rechtevergabe über Workflows und Rollen als auch ein intuitiv bedienbares Warenkorbsystem für Berechtigungsanträge umfasst. Die angebotenen Self-Services der Lösung steigern die Eigenverantwortung der Benutzer spürbar und sorgen damit auch für eine höhere Anwenderzufriedenheit. Die Omada Identity Suite (OIS) stellt zudem Reports bereit, die alle Aspekte der Benutzerverwaltung umfassen. Die Verantwortlichen erfahren beispielsweise, wer wann welche Rechte besessen hat und wer welche Anträge stellt und genehmigt.

Die Software ermöglicht es zudem, die Berechtigungen, aber auch Rollen oder weitere Compliance-Anforderungen zu rezertifizieren, um Fragen des Need-to-Know-Prinzips zu beantworten und so beispielsweise zu klären, ob ein Mitarbeiter noch sämtliche bestehenden Berechtigungen benötigt. Berechtigungen, die ein Verantwortlicher bei einer Rezertifizierung als nicht mehr erforderlich einstuft, werden automatisch in den angebundenen Systemen wie beispielsweise dem Active Directory, SAP, E-Mail-Systemen, Portalen oder Applikationsservern deaktiviert. Abweichungen der Rechte von Standardrollen lassen sich ebenfalls leicht erkennen und entfernen.

Um präventive Sicherheit zu gewährleisten, können IT-Verantwortliche in OIS rollenbasierende Antragsprozesse für Berechtigungen konfigurieren, sodass Compliance-Regeln von Anfang an eingehalten werden.

sollten sie sich jederzeit einen umfassenden Überblick über den aktuellen Stand der Rezertifizierung verschaffen können. Eine leistungsstarke Identity-Management-Lösung sollte darüber hinaus auch die Ergebnisse dieser Überprüfung automatisiert im System umsetzen und beispielsweise nicht mehr benötigte Rechte und Rollen löschen. Nur so haben die verantwortlichen Mitarbeiter in den Fachabteilungen direkten Einfluss auf den Schutz der Unternehmensdaten und letztlich auch auf die Sicherheit ihres Unternehmens. ■

Jutta Cymanek,
Country Manager DACH & Benelux
Omada GmbH

Bedrohungen gezielt abwehren

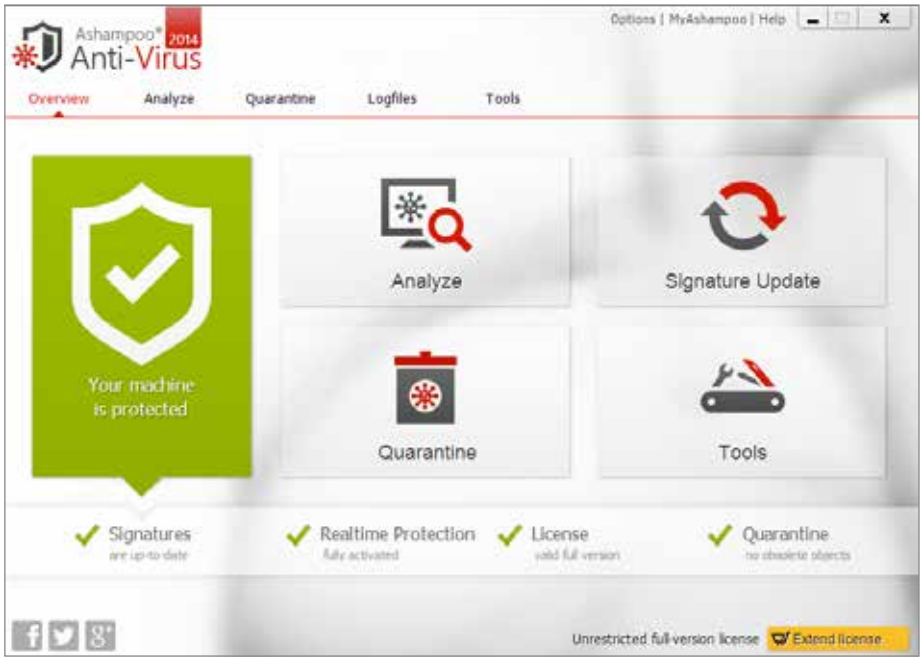
In Schutz investieren

Mehr als 10.000.000 Viren sind laut aktuellen Schätzungen im Umlauf. Antiviren-Lösungen sollten deshalb mehr bieten als nur den Schutz aktualisierter Signaturen. Behaviour Blocker und Echtzeitschutz sorgen dafür, dass Bedrohungen frühzeitig abgewendet werden – noch bevor sie Schaden anrichten können.

Weltweit vertrauen Millionen Nutzer den kostenfreien Antiviren-Produkten bekannter Hersteller. Diese bieten jedoch oftmals nur einen rudimentären Schutz gegen Bedrohungen. Kürzlich hielten die Sicherheitsexperten von AV-Test fest: „Für die Bedrohungen, denen der PC tagtäglich ausgesetzt ist, bieten die Gratis-Virenwächter keinen zuverlässigen Schutz. Selbst bekannte Schadprogramme wurden bei diesem Test nicht erkannt." Die Schutzleistung wurde häufig als „mangelhaft" bewertet. Die getestete Software biete oft nur den Schutz aktualisierter Signaturen, was aufgrund zahlreicher neuer Bedrohungen nicht ausreichend ist. Ausgereifte Lösungen sollten Zusatzmechanismen bieten, wie beispielsweise einen Behaviour Blocker. Damit eine Antiviren-Lösung jedoch dauerhaften Schutz bietet, muss sie kontinuierlich weiterentwickelt und aktualisiert werden, was wiederum Kosten mit sich bringt. Nur Unternehmen, die bereit sind, Geld für ausgereifte Antiviren-Programme auszugeben, können sich auf umfassende Sicherheit verlassen.

Echtzeitschutz und Behaviour Blocker

Herzstück einer jeden effektiven Antiviren-Software sind der Echtzeitschutz und der Behaviour Blocker, die Gefahren frühzeitig abwehren. Die Echtzeitschutz-Technologie bietet Sicherheit ohne jeglichen manuellen Bedienaufwand. Dank des Behaviour Blocker werden die Verhaltensmuster aller Anwendungen laufend analysiert und bei abweichendem Verhalten genauer überprüft. Mit diesem Funktionalität wird der Rechner vor „Zero-Day-



Exploits" geschützt. Ein Zero-Day-Exploit ist ein Angriff, der vor oder am selben Tag erscheint, an dem eine Sicherheitslücke bekannt wird. Dank permanenter Updates ist die Antiviren-Software auf die sich ständig wechselnden Gefahren vorbereitet und bietet somit Schutz gegen nahezu jeden Virus.

Maximale Sicherheit, einfaches Handling

Das Oldenburger Softwareunternehmen Ashampoo bietet mit Ashampoo Anti-Virus 2014 eine moderne Antiviren-Lösung, die die Engines der beiden bekannten Anbieter Bitdefender und Emsisoft nutzt. Dank der täglichen Signaturen-Updates bietet die Lösung von Ashampoo umfassenden und permanenten Schutz. Für diese beiden Engines hat das Ashampoo-Team um Chefentwickler Niki Bugarcici eine intuitive und einfach zu benutzende Bedienoberfläche entwickelt. Neben der Dual-Engine und der benutzerfreundlichen Oberfläche bietet die Software auch weitere nützliche Funktionen. Hierzu zählen unter anderem ein File Wiper-Modul, das Dateien, Ordner oder auch ganze Laufwerke unwiderruflich überschreibt, oder der Internet Cleaner, der den Browser von Cookies, Browser-Caching oder Verlaufslisten befreit. ■

Jan-Gerrit Dickebohm,
Pressesprecher
Ashampoo GmbH & Co. KG


OXFORD
COMPUTER GROUP
Ihr Spezialist für
Identity und Access
Management.
Planen Sie mit uns!
www.oxfordcomputergroup.de

Security & Cloud Computing

Notfall-Management als Management-Aufgabe

Bestens gerüstet für den Fall der Fälle

Notfall-Management erinnert an spektakuläre Szenarien wie Großbrände, Erdbeben und Überschwemmungen. Doch auch ein „kleiner" Notfall kann sich schnell zu einer Krise entwickeln. Deshalb sollten Unternehmen für diese Situationen einen sprichwörtlichen „Plan B" bereithalten.

Der englische Begriff für Notfall-Management lautet „Business Continuity Management" und beschreibt sehr deutlich, worum es geht: Das operative Geschäft einer Organisation muss auch unter dem Einfluss eines großen Schadensereignisses kontrollierbar sein und strukturiert fortgeführt werden können. Notfall-Management ist deshalb eine originäre Management-Aufgabe, betrifft immer die gesamte Organisation und lässt sich nur ganzheitlich umsetzen. Das ist vielen Unternehmenslenkern nicht ausreichend bewusst. Sie sind dafür verantwortlich, Prozesse hierfür aufzusetzen und weiterzuentwickeln und diese in der Praxis mit Leben zu füllen. Dafür muss die Leitung finanzielle Mittel sowie Zeit und personelle Ressourcen bereitstellen. Weitere Hilfsmittel sind Richtlinien, die den organisatorischen Rahmen schaffen. Ferner regelt die Festlegung von Rollen und Verantwortlichkeiten, wer regelmäßig welche Aufgaben übernimmt. All diese Vorgaben bilden die Leitplanken, in denen sich die weiteren Aktivitäten des Notfall-Managements bewegen müssen. Dabei kommt dem IT-Notfall-Management eine besondere Bedeutung zu. Es ist kein singulärer Ansatz, sondern Bestandteil eines ganzheitlichen IT-Managements. So verwundert es nicht, dass alle gängigen Standards und Rahmenwerke Vorgehensweisen für das IT-Notfall-Management bereithalten: ISO 27001 geht im Anhang A.14 darauf ein, ITIL enthält ein eigenes Kapitel über IT Service Continuity Management, und COBIT liefert Handlungsanweisungen in dem Control Objective DSS04.

Mitarbeiter schulen

Das A und O für die erfolgreiche Einführung und Aufrechterhaltung eines Notfall-Management-Prozesses sind sensibilisierte und geschulte Mitarbeiter. Sie haben das nötige Bewusstsein für den Prozess entwickelt und kennen auch die Unterschiede zwischen einem Notfall, einer Krise und einer Katastrophe. Mit einer einmaligen Veranstaltung ist es jedoch nicht getan. Erst regelmäßige Awareness-Maßnahmen schärfen das Bewusstsein für die Notwendigkeit des Notfall-Management-Prozesses, um auch neuen Anforderungen und potenziellen Bedrohungsszenarien gerecht zu werden.

Sind die Risiken bekannt?

Hilfestellung bei der Analyse, wie gut der Notfall-Management-Prozess in einem Unternehmen bereits aufgestellt ist, gibt eine sogenannte Betriebsunterbrechungsanalyse, kurz BIA (Business Impact Analysis). Sie ermittelt, welche Auswirkungen ein Schadensszenario auf die Geschäftsprozesse hat. So lässt sich beispielsweise herausfinden, nach wie vielen Stunden oder Tagen ein Geschäftsbetrieb bereits existenzbedrohend gefährdet ist. Das Unternehmen erfährt zudem, welche Geschäftsprozesse besonders zeitkritisch sind und welche Strategien und Maßnahmen diese wirkungsvoll absichern. Wichtig ist es, die IT-Landschaft vollständig zu erfassen und transparent darzustellen, sodass die gesamte Wirkungskette sichtbar wird.

Experten unterscheiden hierbei zwischen dem Wiederanlauf und der Wiederherstellung nach einem Notfall. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierfür eigens den BSI-Standard 100-4 definiert. Der Wiederanlauf errichtet einen stabilen Notbetrieb mit eventuell eingeschränkter Kapazität. Die Wiederherstellung führt zum ursprünglichen Produktivbetrieb zurück, auch Normalbetrieb genannt. Die im Rahmen der Schadensanalyse festgelegten Schadenskategorien stehen in einem direkten Zusammenhang zum IT-Risiko-Management. Das heißt, hier schlägt die Betriebsunterbrechungsanalyse eine unmittelbare Brücke zu den Sicherheitskonzepten für Anwendungen und Infrastrukturen. Damit wird erneut deutlich, dass Notfall-Management eine ganzheitliche Herangehensweise erfordert.

Dokumentation ist Pflicht

Eine Betriebsunterbrechungsanalyse liefert erste Erkenntnisse über die aktuelle Situation. Sie bildet die Basis dafür, langfristige Strategien und Maßnahmen zur Notfallvorsorge und -bewältigung zu entwickeln. Eine vollständige und strukturierte Dokumentation ist dabei unabdingbar. Sie enthält Notfallpläne und dient als „roter Faden" für die Notfallbewältigung. Mitarbeiter können die darin enthaltenen Checklisten abarbeiten und behalten in Stresssituationen einen kühlen Kopf. Werden die Planung und regelmäßige Durchführung der Tests und Übungen dokumentiert, verinnerlichen die Mitarbeiter beinahe nebenbei auch die Anwendung der Notfall-Management-Prozesse.

Übung macht den Meister

Das einmalige Aufsetzen beispielsweise von Backups und Cluster-Systemen reicht aber nicht aus. Alle Maßnahmen müssen regelmäßig getestet werden, um sicherzustellen, dass sie auch funktionieren. Die besten Notfallpläne und Notfallhandbücher sind nutzlos, wenn sie im Schrank verstauben. Nur eine regelmäßige und kritische Prüfung stellt sicher, dass die Pläne im Notfall praktikabel und aktuell sind. Es gibt ein breites Spektrum an Tests und Übungen, um Maßnahmen zur Notfallvorsorge und -bewältigung auf ihre Effektivität hin zu testen. Dies beginnt idealerweise vor der produktiven Inbetriebnahme der IT-Systeme mit Tests der technischen Vorsorgemaßnahmen. Wichtige Maßnahmen sind darüber hinaus Planbesprechungen, Stabsübungen des Krisenstabs sowie Ernstfall- und Vollübungen. Die notwendige Routine stellt sich allerdings erst ein, wenn alle Mitarbeiter Tests und Übungen regelmäßig durchführen, beispielsweise mit Hilfe eines Test- und Übungsplans.

Plan-Do-Check-Act

Entscheidend für die dauerhaft erfolgreiche Bewältigung von Krisen ist das Bewusstsein, dass Notfall-Management kein Projekt, sondern ein Prozess ist. Das heißt, erst durch regelmäßiges Anwenden und Verbessern bleibt der Notfall-Management-Prozess aufrechterhalten und endet erst, wenn ein anderer Prozess in Kraft tritt. Damit orientiert sich auch das Notfall-Management an dem Plan-Do-Check-Act-Zyklus (PDCA), einem in der Qualitätssicherung etablierten Planungswerkzeug zur Einführung von Verbesserungen. Denn nur die permanente Überprüfung der Notfallvorsorge und -bewältigung im Rahmen von Tests und Übungen (Check) sowie die Optimierung der betreffenden Maßnahmen und Notfallpläne (Act) führen nachhaltig und erfolgreich zum Ziel: bestens gerüstet zu sein für den Fall der Fälle. ■

Dipl.-Ing. Alfons Marx, Teamleiter Security, DQS-Auditor, Kompetenzteam Information Security Management bei der Materna GmbH

Heiko Wurster, zertifizierter Lead Auditor BS 25999 und Senior Consultant bei der Materna GmbH

12-Punkte-Sicherheitstopologie als Basis für maximalen Schutz und Compliance

Cloud Computing – strukturiert, standardisiert und sicher

Analysten überschlagen sich mit ihren Studien zur Zukunft des Cloud Computing. Gleichzeitig bremsen jedoch Sicherheitsbedenken die Cloud-Euphorie. Dabei sind Ängste vor potentiellen Risiken verständlich, denn die Zahl der Attacken auf IT-Systeme steigt täglich.

Um externen wie internen Risiken des Cloud Computing zu begegnen, müssen Unternehmen das Thema ICT-Sicherheit ganzheitlich angehen, alle möglichen Gefahrenquellen prüfen und Schutzmaßnahmen strukturiert einführen. T-Systems hat dafür eine Sicherheitstopologie mit zwölf Aufgaben entworfen, die jedes Unternehmen im Interesse der Sicherheit für die eigenen Daten und Applikationen in der (Private) Cloud beachten sollte. Gleichzeitig unterstützt und flankiert ein strukturierter, standardisierter Weg in die Cloud diese Sicherheitsmaßnahmen.

Cloud Computing braucht (k)eine neue Sicherheit

Cloud-Anwender haben vielfältige externe Anforderungen und „Compliance"-Vorgaben zu berücksichtigen. Diese stellen keine vollständig neuen Herausforderungen dar. Jedoch verschieben sich Schwerpunkte sowie die Wichtigkeit einiger Aspekte. Hierzu ist ein umfassender Blick erforderlich. Deutlich wird dies besonders bei Collaboration-Lösungen. Bereits während der Konzeption sind Sicherheitsaspekte auf unterschiedlichen Ebenen zu berücksichtigen: Auf technischer Ebene (2-6) ist die Absicherung der Infrastruktur vor Fremdeinwirkungen, z. B. über die Abschirmung des Datenverkehrs via VPN, eine ausfallsichere Datenspeicherung oder Mobile Security, notwendig. Auf Nutzerebene geht es bei Ressourcen und Anwendungen um digitale Identitäten und ein abgestuftes Zugangs- und Berechtigungsmanagement (1). Auf der prozessual-operativen Ebene muss die Sicherheit in die Geschäftsprozesse integriert und mit Zielen hinterlegt werden (7-9). Das übergreifende Security-Management sollte organisatorisch als Teil des operativen Risikomanagements verankert sein und unternehmensweite Richtlinien für Informationssicherheit, Governance und Compliance formulieren (11-12). All dies erfordert eine übergreifende und gegliederte Vorgehensweise.

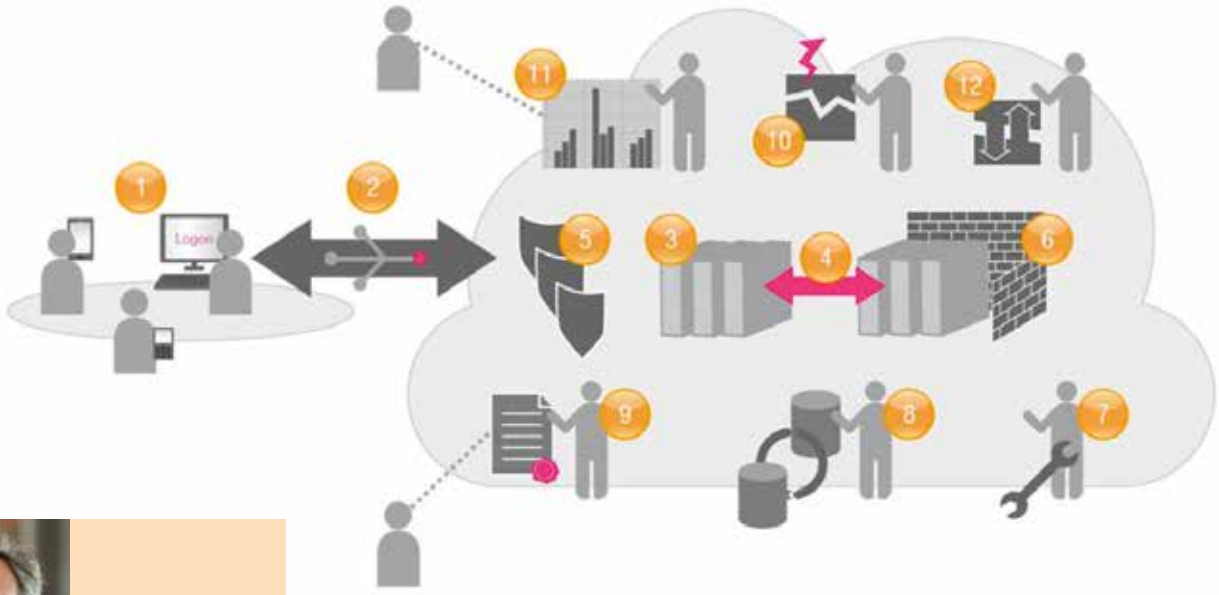
Strukturiert in die Cloud

Damit Cloud Computing ein hohes Sicherheitsniveau bietet, sollten Unternehmen sehr genau hinschauen, welchen Service sie von welchem Cloud-Anbieter beziehen wollen.

Hierzu empfiehlt sich eine strukturierte und standardisierte Vorgehensweise:

1. Aufbau einer businessorientierten Cloud-Strategie
2. Analyse der Applikations- und Prozesslandschaft
3. Bedarfs- und prozessorientierte Auswahl der Cloud-Services
4. Erstellung einer Cloud-Roadmap
5. Cloud-Transformation, Migration und Integration

Neben den technischen und businessorientierten Anforderungen sind die Anforderungen an den Datenschutz ebenso ernst zu nehmen wie die Mitbestimmungsrechte seitens der Arbeitnehmervertretungen. Auch die künftigen Anwender der Collaboration-Lösung sind frühzeitig einzubinden, entscheiden sie doch mit ihrem Nutzungsverhalten über deren Erfolg und Profitabilität. ■



Dr. Michael Pauly, Consultant Dynamic Services & Cloud Computing, T-Systems International GmbH

Quellen:

Tobias Höllwarth (Hrsg.): Der Weg in die Cloud. 2. Auflage, mitp Verlag, Heidelberg, München, Landberg, Frechen, Hamburg, 2012.

Whitepaper Cloud Security, T-Systems, 2012.

Whitepaper Collaboration: Innovative Formen der Zusammenarbeit, T-Systems, 2013.

M. Rath, R. Sponholz: IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen, Verlag Erich Schmidt, Berlin, 2009.

Compliance-konformes Enterprise Content Management in der Cloud

Cloud Computing und Compliance in Symbiose

Cloud Computing und Compliance in Symbiose? Geht das wirklich? Nicht nur theoretisch, sondern auch in der realen Arbeitswelt? Und das ohne hohe Kosten oder Einbußen bei der Performance oder Funktionalität aller gängigen Office-Anwendungen?

Nach wie vor herrscht die Meinung, dass sich Cloud Computing und Compliance gegenseitig ausschließen. MERENTIS tritt den Gegenbeweis an. Der Begriff Cloud geht oft mit den Attributen der Unbekanntheit der tatsächlichen Datenspeicherung oder mangelnder Rechtskonformität einher. Gleichzeitig wird die Compliance-Erfüllung gerne mit einer On-premise-IT-Administration und einem hohen finanziellen Aufwand gleichgesetzt. Bei steigendem Kostendruck und stets komplexer werdenden rechtlichen Vorgaben müssen Unternehmen sich daher laufend nach neuen und innovativen Möglichkeiten umsehen, diese beiden wichtigen Faktoren so optimal wie möglich miteinander zu kombinieren.

Technisches Consulting, Compliance-Beratung und Projektumsetzung in einem

Oft findet man Berater, die entweder nur den technischen oder nur den rechtlichen Aspekt des Enterprise Content Managements in der Cloud anbieten können, so dass zwei externe Partner engagiert werden müssen, um beide Bereiche vollständig abdecken zu können. MERENTIS bietet eine Kombination aus technischem Consulting und Compliance-Beratung. Dank langjähriger Erfahrung und zahlreicher, erfolgreich umgesetzter ECM-Projekte gehen MERENTIS Consult und MERENTIS DataSec routiniert an neue Projekte heran. So entsteht eine vollständig abgesicherte Lösung, die sowohl die technische Stabilität als auch die zertifizierte Rechtssicherheit einer Dokumentenverwaltung gewähr-

leistet. Nach einer Analyse der ECM-Landschaft und einer Klassifizierung aller Unternehmensdokumente wird eine sinnvolle Dimensionierung der Verteilung von Cloud- und On-premise-Komponenten erstellt. Dies hat zum Ziel, das Optimum zwischen Kosteneffizienz auf der einen Seite und einhundertprozentiger Rechtskonformität der Unternehmensdaten auf der anderen Seite zu erreichen. Im Zuge dessen wird ein Compliance-konformes ECM auf Basis von Windows Azure und Office 365 aufgebaut.

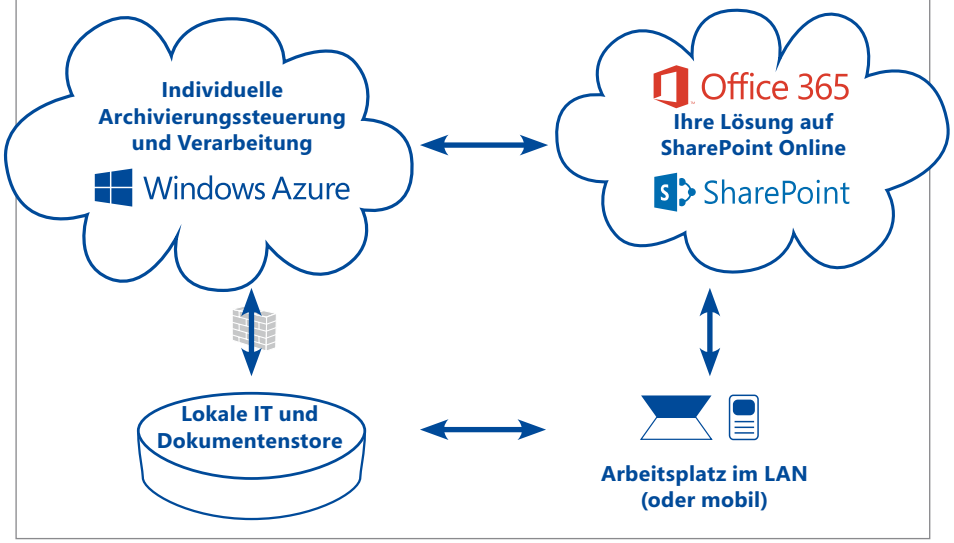
Arbeiten in der Cloud – Archivierung im deutschen Rechenzentrum

Der wichtigste Aspekt der Lösung ist die Kombination aus der Sicherheit von On-premise-Archivierung und dem Einsparpotenzial der Cloud-Nutzung. Dabei werden die Dokumente in einem deutschen Rechenzentrum abgelegt – direkt im eigenen Haus oder per Hosting bei einem Drittanbieter. Dazu wird in SharePoint Online ein (für den Nutzer als solcher nicht erkennbarer) Link hinterlegt, der direkt zum lokal abgelegten Dokument führt. Das heißt, es findet zu keinem Zeitpunkt ein Dokumenten-Upload in die Cloud statt, alle sensiblen Daten werden direkt im Rechenzentrum gespeichert und sind für die User mittels Authentifizierung über SharePoint jederzeit zugänglich. Die Nutzer arbeiten somit transparent in SharePoint Online mit den Unterlagen und können alle Funktionen des Tools in vollem Umfang nutzen.

Die Vorteile des Cloud Computing optimal nutzen

Auf diese Weise können alle Vorteile des Cloud Computing wie eine standortunabhängige Nutzung aller Daten, die Auslagerung der IT-Administration sowie Kosteneinsparungen, mobiler Zugriff durch den Außendienst und die von Windows Azure garantierte Verfügbarkeit genutzt werden, ohne Unternehmensdaten in der Cloud ablegen zu müssen. Diese Lösung funktioniert zu fast 100 Prozent cloudorientiert, wobei die Administration zum größten Teil an Microsoft übergeht und die eigene, interne IT stark entlastet wird.

Übersicht Lösungskomponenten



Hohes Maß an Sicherheit dank zweifacher Authentifizierung

Um unternehmensinterne Daten vor dem Zugriff Unbefugter zu sichern, erfolgt die Authentifizierung für jedes sensible Dokument in zwei Berechtigungsschritten. Der Benutzer meldet sich im ersten Schritt über seinen SharePoint-Account an. Danach kann er im zweiten Schritt die einzelnen Dokumente nur durch eine weitere Authentifizierung öffnen und/oder bearbeiten. Somit wird der Zugriff auf sensible oder personenbezogene Daten nur für berechtigte Personen möglich.

Compliance garantiert

Im Rahmen der Vorab-Analyse wird ein detaillierter und qualifizierter Sicherheitsbericht erstellt. Dieser zeigt bestehende Risiken auf, die dann im Rahmen der Lösungsumsetzung eliminiert werden. Jede einzelne Komponente der Lösung ist gemäß rechtlichen Revisionsrichtlinien zertifiziert und erfüllt folglich jede Qualitäts- und Compliance-Anforderung – unabhängig davon, ob gemäß deutschem oder europäischem Recht.

Sicherer mobiler Zugriff

Die Lösung ist so konfiguriert, dass sie von allen gängigen mobilen Endgeräten genutzt werden kann – ohne dabei an Sicherheit oder Funktionalität einzubüßen. Sowohl die zweifache Authentifizierung als auch der Transfer über SharePoint Online funktionieren genauso wie bei einem Client-Arbeitsplatz. ■

Vorteile der Lösung auf einen Blick

- Nutzung von Microsoft SharePoint in der Cloud
- Archivierung der Unternehmensdaten in einem deutschen Rechenzentrum
- Erfüllung aller Compliance-Vorgaben
- On-premise-IT und Betriebsaufwand werden auf ein Minimum beschränkt
- Höchstmaß an Sicherheit dank zweifacher Authentifizierung
- Möglichkeit des sicheren, mobilen Zugriffs auf Dokumente
- Die Lösung arbeitet zu 100 Prozent cloudorientiert
- Verbindung von technischem Consulting, Compliance-Beratung und Projektumsetzung
- Individuelle, auf Unternehmensanforderungen zugeschnittene Lösung

Thorsten Fiedler,
EIM- und SharePoint-Architekt,
Geschäftsführer
MERENTIS Consult GmbH

Larissa Schwarz,
Rechtsanwältin,
Leiterin Fachbereich Datenschutz
MERENTIS DataSec GmbH

Beiersdorf hat höchste Qualitätsansprüche bei der eigenen IT-Sicherheit

Im Sichtflug

Die Beiersdorf Shared Services GmbH hat für den Beiersdorf-Konzern eine zentrale Qualitätssicherung für Malware-Protection sowie Patch-Management eingeführt und dadurch das weltweite Niveau seiner IT-Sicherheit nachweislich gesteigert.

Beiersdorf steht unter anderem mit seiner Traditionsmarke NIVEA weltweit für höchste Kompetenz in Sachen Haut- und Körperpflege. Als eine der Hauptzutaten seines Erfolgsrezeptes betrachtet Beiersdorf die Nähe zum Kunden und das grundlegende Verständnis individueller Ansprüche. Für Marktnähe sorgen unter anderem lokale Gesellschaften an über 80 Standorten rund um den Globus. Die Hoheit über die globale IT-Infrastruktur hat Beiersdorf der Beiersdorf Shared Services GmbH (BSS) übertragen, einer eigenständigen Tochtergesellschaft mit Sitz in Hamburg. BSS hat den Auftrag, das Wachstum von Beiersdorf durch die Bereitstellung von Buchhaltungs- sowie IT-Dienstleistungen zu unterstützen. Der Schutz der Daten und die Aufrechterhaltung des IT-Betriebs sind dabei von zentraler Bedeutung. Jörg Meier, Manager Platforms and Infrastructure Applications, und sein 24-köpfiges Team widmen sich von der Hansestadt aus dieser gewaltigen Aufgabe. Mit der Einführung eines Monitoring-Systems für die IT-Sicherheitssysteme hat das BSS-Team nun die notwendige Transparenz geschaffen, um wirksam an der Qualität der IT-Sicherheit arbeiten zu können.

Komplexes Netzwerk

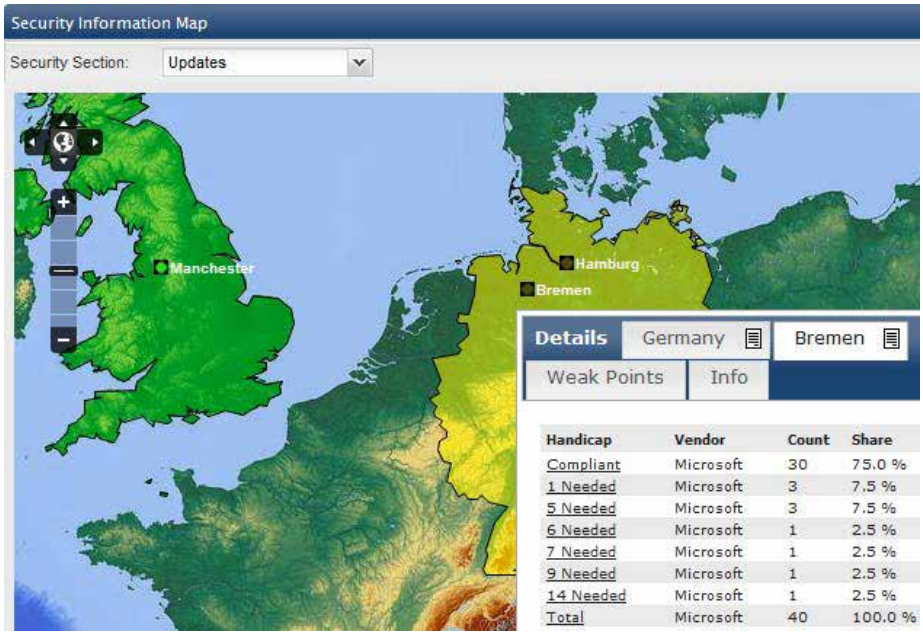
Zu den Aufgaben des Teams rund um Jörg Meier gehören unter anderem das weltweite Server-Management und die Bereitstellung der Rechner für die Mitarbeiter. Etwa 200 Microsoft Exchange-, SharePoint- und SQL-Server gehören ebenso zur globalen IT-Architektur wie die circa 14.000 Clients an den Beiersdorf-Standorten. Bis zum Jahr 2010 setzte BSS im Bereich Malware-Schutz durchgehend auf Produkte von McAfee, danach erfolgte eine Umstellung auf Microsoft Forefront-Lösungen für Clients und Server. Microsoft WSUS kümmert sich seit vielen Jahren um das Patch-Management bei Servern. Die Einführung von Microsoft SCCM für das Patch-Management auf den Clients wurde vor Kurzem abgeschlossen. „Zu McAfee-Zeiten versorgte uns der McAfee E-Policy Orchestrator mit Informationen zum Sicherheitsstatus der AV-geschützten Systeme", erklärt Jörg Meier. „WSUS und SCCM zeigten uns den Patch-Status für die einzelnen Clients." Berichte erfolgten an den Security Officer von BSS, der zudem unabhängig von Jörg Meiers Team mittels eines Nessus-Scanners Prüfungen der Schwachstellen vornahm.

Schwachstelle Intransparenz

„Im Nachhinein muss ich sagen, dass wir damals viele Dinge nicht gesehen haben", gibt der Manager zu. Vor allem übergreifende Auswertungen zur Sicherheitslage waren demnach nicht möglich. „War beispielsweise auf einem System die Installation des McAfee-Agents fehlgeschlagen, so tauchte dieser in der Management-Konsole einfach nicht auf. Wir hatten keine Möglichkeit zur unabhängigen Prüfung beziehungsweise Qualitätssicherung für unsere IT-Sicherheitssysteme." Beim Patch-Management stellte sich die Situation ähnlich dar. Die Einhaltung der strengen Vorgaben – Patches mit der Bewertung „critical" müssen demnach weltweit unverzüglich, andere wichtige Patches nach der Prüfung durch ein BSS-Gremium innerhalb von zwei Wochen ausgerollt sein – konnte nur bei den Systemen überprüft werden, die MS WSUS beziehungsweise SCCM registriert hatte. Server oder Clients, die nicht an das AV- oder Patch-Management angeschlossen waren, wurden zu blinden Flecken im Netzwerk, zu nicht identifizierbaren Schwachstellen. „Es konnte also vorkommen, dass ein Rechner laut McAfee optimal geschützt, aber auf Patch-Seite völlig offen war", erklärt Jörg Meier. Bei Angaben zum Security Level oder auch bei Auswertungen zu einzelnen Rollouts konnte das Team keine unabhängige Prüfung der Angaben der Sicherheitssysteme durchführen.

Konsolidierung der Informationen

Vor etwa drei Jahren entschied die Abteilung um Jörg Meier, das unabhängige Nebenher der Sicherheitssysteme zu beenden. „Wir wollten auf einen Blick erkennen können, wie es um den Sicherheitsstatus eines Systems, einer Systemgruppe oder auch des gesamten Netzwerks bestellt ist", sagt Jörg Meier. BSS wollte dazu auf eine bewährte Monitoring-Lösung setzen, die keine Eigenentwicklungen erforderte und trotzdem so flexibel war, um mit den hohen Ansprüchen von BSS Schritt zu halten. Ein bereits damals angedachter Wechsel von McAfee auf Microsoft-Sicherheitslösungen durfte auch für eine übergreifende Security Level Management-Software keine Hürde darstellen. Die zentrale Anforderung bei der Auswahl einer Lösung war deren Fähigkeit, übergreifende Auswertungen bereitzustellen, und das in Echtzeit und webbasiert. Mitarbeiter sollten sowohl von ihren Rechnern als auch mobil jederzeit darauf zugreifen und sich aussagekräftige Statusberichte für Meetings ausgeben lassen können. BSS entschied sich schließlich für das AMPEG Security Lighthouse, eine Security Level Management-Lösung der AMPEG GmbH.



In der Security Information Map lässt sich der aktuelle Sicherheitsstatus in Echtzeit einsehen.

Verlorene Systeme

Die Inbetriebnahme des Monitorings war nach einer Woche abgeschlossen. Dafür setzte das Projektteam den Security Lighthouse-Server auf und schloss mittels der „Kollektoren" des Systems die Management-Konsolen von McAfee, MS WSUS, MS SCCM sowie das MS Active Directory an die AMPEG-Lösung an. Nach einer eintägigen Schulung des BSS-Teams wurde das Monitoring das erste Mal eingeschaltet. „Schon beim ersten Lauf wurde der Wert der Lösung deutlich: Tatsächlich waren etwa zehn Prozent unserer Rechner weltweit nur an jeweils ein Sicherheitssystem angeschlossen. Zehn Prozent erhielten also Virenpattern aber keine Patches und umgekehrt", so Jörg Meier. Durch die Zusammenführung der Daten aus vier Systemen konnten diese Schwachstellen unmittelbar identifiziert werden. „Zehn Prozent sind unserer Erfahrung nach noch ein sehr guter Wert", kommentiert Michael Hänsel, Projektmanager bei AMPEG. „BSS kann man guten Gewissens als einen Musterbetrieb in Sachen IT-Sicherheit bezeichnen, da BSS auch vor der Installation unseres Systems identifizierbare Sicherheitslücken konsequent geschlossen hat. Wir haben auch schon Netzwerke gesehen, bei denen die Quote deutlich schlechter lag." Mit der Aktivierung des Security Lighthouse konnte das BSS-Team mit der Behebung der Schwachstellen beginnen.

Ende des „Blindflugs"

Die Umstellung von McAfee auf MS Forefront Endpoint Protection im September 2010 beeinträchtigte den laufenden Betrieb nicht. AMPEG hatte den Forefront-Kollektor vorbereitet, sodass am Tag des Systemwechsels sofort Daten aus MS Forefront in das Monitoring-Tool fließen konnten. Die Monitoring-Software zeigt in ihrem Dashboard in Ampelfarben den korrelierten Sicherheitsstatus von Ländern, Standorten, definierten Systemgruppen oder Einzelsystemen an. Die Signalfarben Rot, Gelb oder Grün ergeben sich aus den gewählten Grenz- und Schwellenwerten, die BSS festgelegt hat. Beim Patch-Management wird der Sicherheitsstatus eines Standortes nur dann in Grün angezeigt, wenn dort auf allen Systemen alle „critical"- und „security"-Patches installiert wurden. Für Standorte, die mit Gelb oder Rot markiert sind, liefert die Lösung Detailinformationen zu den Systemen mit Angaben zu den fehlenden Patterns oder Patches. Die Informationen zum Sicherheitsstatus können von den betreffenden Standortverantwortlichen genutzt werden. Dashboard wie Detailanalysen können webbasiert am PC-Arbeitsplatz, aber auch mobil per iPad abgerufen werden. „Wenn ich morgens meine Security Information Map aufrufe, ist meist noch sehr viel Rot zu sehen, weil das aktuelle Virenpattern noch nicht verteilt ist. Es macht Spaß, zu verfolgen, wie die Standorte von Osten nach Westen im Laufe des Tages auf Grün wechseln", so Jörg Meier.

Ausweitung der Transparenz

BSS arbeitet kontinuierlich an der Verbesserung der IT-Sicherheit für die Beiersdorf-IT-Landschaft. Das nächste Projekt steht bereits ins Haus: die Identifizierung von Software, die sich Mitarbeiter selbst auf ihren Rechnern installiert haben und die gegebenenfalls ebenfalls Bedrohungen für die IT-Sicherheit mit sich bringt. Das können nicht freigegebene Betriebssysteme sein oder auch unerwünschte Programme wie Apples iCloud oder der Dienst „Dropbox", die immer populärer werden. Für freigegebene Programme muss mittels eines professionellen Update-Managements ebenfalls der Entstehung von Schwachstellen entgegengewirkt werden. Wie beim Pattern- und Patch-Management ist Transparenz hier der erste Schritt für ein wirksames Security Level Management. Die Analyse des Software-Inventory mit dem Security Lighthouse wird BSS unterstützen, diese Transparenz herzustellen.

Den Status der bis heute realisierten Qualitätssicherung für die IT-Sicherheit beurteilt der Manager Platforms and Infrastructure Applications positiv: „Aktuell sprechen wir wöchentlich mit unserem Security Officer. Dabei sehen wir uns weiterhin stichprobenartig Auswertungen seines Vulnerability Scanners an. Der Unterschied zu früheren Meetings ist, dass er uns mit seinen Ergebnissen nicht mehr überrascht. Wir sehen im Detail dieselben Schwachstellen wie er und haben zudem den übergreifenden Blick auf alle Systeme. Diese Gesamtsicht in Bezug auf den Sicherheitsstatus bei Beiersdorf weltweit ist für mich der wertvollste Aspekt dieses Projektes", fasst Jörg Meier zusammen. ■

Jörg Meier,
Manager Platforms and Infrastructure Applications
Beiersdorf Shared Services

Agnes Graf,
Geschäftsführerin und Mitgründerin AMPEG

infoWAN schafft standardisierte Prozesse bei der itsc GmbH in Hannover

Mit durchdachtem User Provisioning effizienter und sicherer arbeiten

Identity und Access Management ist heute eine der zeitaufwändigsten Aufgaben für IT-Verantwortliche und Administratoren in Unternehmen, deren Komplexität nicht zu unterschätzen ist. Administratoren müssen deshalb effektive und sichere Lösungen aufsetzen, die Single-Sign-On, Self-Services für Passwort-Resets und konsistentes Passwort-Management in einem durchgängigen, unternehmensweiten Prozess ermöglichen. Nur damit ist gewährleistet, dass die Administratoren und Helpdesk-Mitarbeiter in den Unternehmen entlastet werden und die Produktivität der Anwender nicht sinkt.

Als Universaldienstleister für gesetzliche Krankenkassen betreut die itsc GmbH in Hannover rund 80 Betriebskrankenkassen, Ersatzkrankenkassen sowie Innungskrankenkassen mit insgesamt rund 5.500.000 Mitgliedern. Das im Jahr 1999 gegründete Unternehmen beschäftigt heute ca. 400 Mitarbeiter an elf Standorten und bietet seinen Kunden ein umfassendes Portfolio an IT-Dienstleistungen. Hierzu zählen unter anderem der Rechenzentrumsbetrieb inklusive der erforderlichen Wartungsleistungen, die Realisierung von WTS-Arbeitsplätzen sowie die Bereitstellung von Standard-Softwareanwendungen für Krankenkassen und individuell zugeschnittenen Lösungen. Als Data-Center dieser Größenordnung haben Informationssicherheit sowie effiziente und durchgängige Prozesse für die itsc-Unternehmensgruppe deshalb einen sehr hohen Stellenwert.

Den Aufwand senken, die Sicherheit erhöhen

Den Umstieg auf das neue Informationssystem für Krankenversicherungen iskv_21c nahm itsc zum Anlass, auch das Identity und Access Management zu verbessern. Bisher gab es für das Benutzer- und Zugriffsmanagement keine übergreifenden und einheitlichen Strukturen. Die Prozesse waren in diesem Kontext nicht automatisiert und standardisiert. Dies fördert wiederum die Fehleranfälligkeit. „Wir verfügen über eine heterogene IT-Infrastruktur. Die Anwender des Kunden wie auch die Mitarbeiter haben jeweils mehrere User-Accounts für die verschiedenen Systeme und Anwendungen. Damit entsteht natürlich auch ein sehr hoher Aufwand für die Administration", erläutert Mike Behrens, Fachbereichsleiter im Bereich Server Backend Systeme bei der itsc System-Service GmbH & Co. KG. „Deshalb möchten wir ein IAM-System schaffen, in dem jeder User lediglich einen Account für seine verschiedenen Systeme erhält und durch die Nutzung von Self-Services bestimmte Prozesse selbst abwickeln kann." Um das Identity und Access Management für die Anwender der Kunden sowie für die eigenen Mitarbeiter effizienter zu gestalten, suchte das verantwortliche IT-Team rund um Mike Behrens eine Lösung, die das bestehende Passwort-Management mit dem Microsoft Forefront Identity Manager erweitert. Der Microsoft Forefront Identity Manager (FIM) ist eine Lösung für die Verwaltung von Benutzeridentitäten und der dazugehörigen Berechtigungen über den gesamten Lebenszyklus hinweg. Die Lösung bietet Identitätssynchronisierung, Zertifikats- und Kennwortverwaltung sowie User Provisioning.

Herausforderungen in Microsoft-Umgebungen

Das Passwort-Management mit dem Microsoft Forefront Identity Manager sieht vor, dass der Mitarbeiter im Unternehmen ein Passwort erhält, und der Administrator unter anderem Folgendes definiert:

- Wie viele Versuche hat der Mitarbeiter, um sich anzumelden?
- Wie lange muss der Mitarbeiter warten, bis er sich wieder anmelden kann?
- Wann wird der Mitarbeiter vom System gesperrt?

In einer Netzwerk-Umgebung mit dem Forefront Identity Manager ist grundsätzlich ein Passwort-Reset über Sozialfragen

(Mädchenname der Mutter, Lieblingsstofftier etc.) möglich. Dennoch kommt es hierbei in rund fünf von fünfzig Fällen dazu, dass der Anwender den Helpdesk kontaktieren muss, damit er im Portal und im Windows-Netzwerk wieder entsperrt wird. Ist der Mitarbeiter erst einmal gesperrt, kann in der Regel nur ein Dritter, der über die entsprechenden Berechtigungen verfügt, diesen wieder entsperren. Hierbei gilt es zu bedenken, dass ein Berechtigter die Zugriffsrechte eines Mitarbeiters auch missbrauchen könnte. Kann ein Mitarbeiter sich nicht anmelden, geht er im Normalfall davon aus, dass er sich vertippt hat oder gesperrt ist. Zu einer Hinterfragung der Rechtmäßigkeit oder einer Ursachenforschung kommt es nach solch einem Vorfall meist nicht.

Aufgaben und Workflows definieren

Besonders wichtig bei der Umsetzung eines IAM-Projekts ist die Definition der Workflows und Prozesse: Wer legt User an? Was darf ein Anwender selbst unternehmen? Wie werden ausgeschiedene Mitarbeiter sicher und verlässlich gelöscht? Welche Regeln gelten für zeitlich befristete Anwenderkonten? Die eigentliche technische Umsetzung tritt dabei zunächst in den Hintergrund. Sind alle Prozesse definiert und damit transparent für die verantwortlichen Mitarbeiter, hat ein Unternehmen auch die Basis für ein dauerhaft effizientes User Provisioning geschaffen. „Wichtig für die Umsetzung eines IAM-Projekts ist vor allem die Planungs- und Konzeptionsphase. Hierzu zählt insbesondere die Festlegung der wichtigsten Ziele, die Prüfung und Validierung aller im Unternehmen genutzten Systeme, die in ein integriertes IAM-System eingebunden werden müssen, sowie eine mehrstufige, strukturierte Umsetzung. Mit dem Proof-of-Concept konnten wir die Machbarkeit und Durchführbarkeit des Projekts nachweisen und haben damit Planungs- und Investitionssicherheit“, kommentiert Mike Behrens von itsc.

Mehr Effizienz, mehr Flexibilität, mehr Sicherheit

Zusammen mit dem etablierten IT-Dienstleistungsunternehmen infoWAN – Henry Schleichardt zeichnete verantwortlich für Design und Implementierung – konzeptionierten die IT-Verantwortlichen von itsc ein Portal, das die bestehende Lösung für Microsoft FIM erweitert. Mit diesem neuen Portal lassen sich die rund 400 Anwenderkonten erstellen, pflegen und auch wieder zuverlässig löschen. Dabei ist dieses Management-Frontend mehrstufig aufgebaut: Dank dieses Portals können beispielsweise auch Anwender selbst ihr Passwort zurücksetzen. Dies entlastet die Mitarbeiter am Helpdesk erheblich. Denn nun reicht es aus, wenn sie in der nächsten Stufe eingreifen: im Falle von Rückfragen oder Problemen bei der Umsetzung durch den User. Das spart Zeit und Aufwand für die IT-Verantwortlichen. Da dieses Frontend von den Anwendungssystemen entkoppelt ist, wird sichergestellt, dass Endanwender und auch Helpdesk-Mitarbeiter dabei keinen direkten Zugriff auf die Endsysteme erhalten. Dieser automatisierte Prozess des Passwort-Resets ist nicht nur auf Microsoft-Lösungen beschränkt, sondern kann auch für die Produkte von Drittanbietern genutzt werden. Zudem ist es möglich, andere Sicherheitslösungen für die Authentifizierung einzubinden und damit beispielsweise eine SMS mit einer ID für die Entsperrung an ein mobiles Endgerät zu schicken. Darüber hinaus ermöglicht es die von infoWAN erweiterte Lösung, dem Anwender eine Nachricht per E-Mail zu senden, wenn es zu einem Passwort-Reset kommt. Somit hat der User die Kontrolle über seine Passwörter und kann erkennen, wenn ein unbefugter Dritter sein Passwort genutzt hat. Da die erweiterte Lösung von infoWAN alle Aktionen dokumentiert und in einer SQL-Datenbank hinterlegt, ist auch ein umfassendes Reporting möglich. „Unsere Zielsetzung ist es, das User Provisioning dauerhaft zu optimieren, den Aufwand für diese Aufgaben deutlich zu reduzieren, die Prozesse zu standardisieren und zu einem möglichst hohen Grad zu automatisieren. Zusammen mit infoWAN konnten wir dies realisieren“, ergänzt Mike Behrens von itsc. „Zudem möchten wir künftig eine umfassende Protokollierung und Dokumentation über die Verwaltung der Benutzer und deren Rechte erreichen. Dank der Dokumentation und statistischen Auswertungen erhalten wir einen umfassenden Überblick über die Ist-Situation, die Aufwendungen für das User Provisioning sowie jegliche Erstellung, Pflege und Löschung von Anwenderkonten.“ ■

„Das Rezept für effizientes und sicheres Identity und Access Management heißt Standardisieren und Automatisieren.“

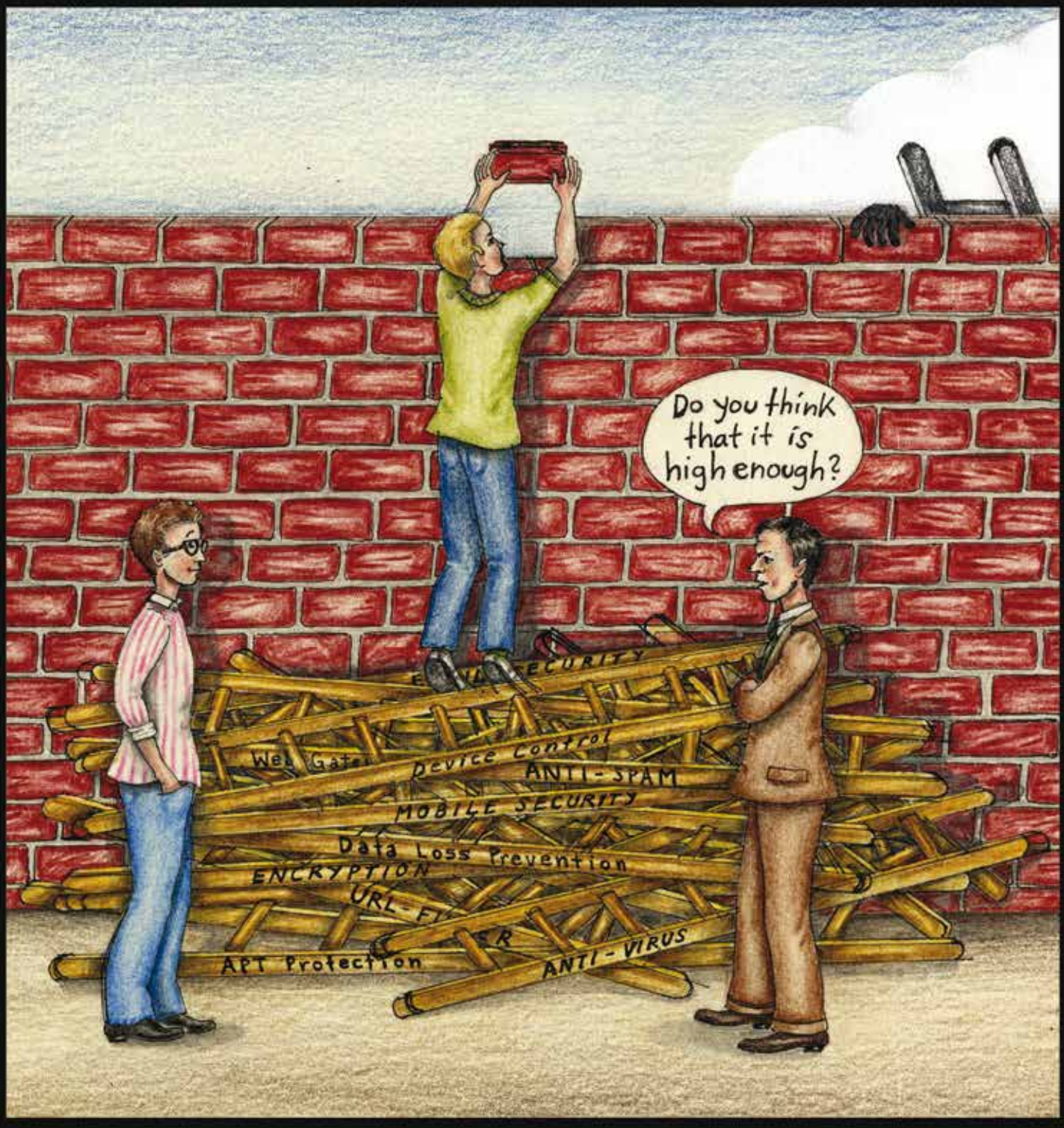
Mike Behrens
itsc System-Service GmbH & Co. KG

infoWAN Datenkommunikation GmbH

Die infoWAN Datenkommunikation GmbH ist ein Dienstleistungsunternehmen mit Sitz auf dem Microsoft Campus in Unterschleißheim bei München. Das im Jahr 1996 von Geschäftsführer Lars Riehn gegründete Unternehmen ist heute auch an den Standorten Regensburg, Frankfurt am Main und Jena mit eigenen Niederlassungen vertreten. infoWAN bietet ein umfassendes Dienstleistungsportfolio für die Planung, den Aufbau und den Betrieb von leistungsstarken und sicheren IT-Infrastrukturen. Als Microsoft Gold Certified Partner ist infoWAN spezialisiert auf die Lösungen des etablierten amerikanischen Softwareanbieters. Zu den fokussierten Microsoft-Technologien zählen die Server- und Client-Betriebssysteme, Microsoft System Center sowie alle Lösungen für das Kommunikations- und Informationsmanagement wie Microsoft Exchange, Microsoft SharePoint, Microsoft Lync und Microsoft Office 365. Die IT-Experten des Unternehmens verfügen über umfassendes Know-how in den Bereichen Infrastruktur-Management, Unified Communications & Collaboration, Cloud Computing, Mobile Computing, Virtualisierung, Archivierung, Backup & Recovery sowie Security.

Henry Schleichardt,
Senior Consultant
infoWAN Datenkommunikation GmbH

It doesn't matter how many IT-Security solutions you are using.



If you don't use them to maximum effect,
your security level will never be high enough.

AMPEG Security Lighthouse Security Level Management

www.security-lighthouse.de

Sicher und flexibel mit Avanade und Microsoft

„Polizei-Cloud" des Landes Rheinland-Pfalz BSI-zertifiziert

Unter dem Druck der Schuldenbremse und der umfassenden Sparmaßnahmen von Bund und Ländern suchen öffentliche IT-Dienstleister nach Einsparpotenzialen, ohne jedoch ihre aktuellen Serviceleistungen zu reduzieren – so auch der Landesbetrieb Daten und Information (LDI) des Landes Rheinland-Pfalz.

Auf den ersten Blick scheinen die beiden Ziele nicht vereinbar zu sein. Diese wurden jedoch durch die Entscheidung des LDI zugunsten einer konsequenten Virtualisierung der bestehenden Systeme auf einer optimierten und automatisierten Cloud-Infrastruktur vereint. So entstand eine moderne und kosteneffiziente Lösung für die öffentliche Verwaltung des Landes Rheinland-Pfalz.

Von der Konzeptionsphase bis hin zur Umsetzung dieser Cloud-Umgebung unterstützte Avanade den LDI mit Fachwissen und Erfahrung aus der Umsetzung komplexer Cloud-Projekte. Als Basis diente Microsoft Server Hyper-V 2008 R2 mit den folgenden System-Center-Produkten: Virtual Machine Manager 2008 R2, Virtual Machine Manager Self Service Portal 2.0, Operations Manager 2007 R2, Configuration Manager 2007 R3, Data Protection Manager 2010 sowie Opalis.

Höchste Anforderungen an die Sicherheit

Ein besonderes Augenmerk wurde auf die Sicherheit bei der Entwicklung der Systemarchitektur gelegt, um die hohen Anforderungen der Verwaltung, beispielsweise der Polizei, erfüllen zu können. Zudem strebte der LDI eine Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) an. Das Engagement hinsichtlich Sicherheit zahlt sich jetzt aus: Im Juli 2013 erhielt die sogenannte „Polizei-Cloud" des LDI das ISO 27001 Siegel auf der Basis von IT-Grundschutz. Diese erstmals in Deutschland erteilte Zertifizierung für einen Cloud-Service ist der konsequenten Umsetzung der Richtlinien „Virtualisierung des IT-Grundschutzkataloges des BSI", der LDI-Sicherheitspolicy sowie dem LDI-Maßnahmenkatalog geschuldet, der vom IT-Grundschutzkatalog abgeleitet ist.

Microsoft Windows Hyper-V als Kernstück

Das Kernstück der „Polizei-Cloud" stellt dabei die Microsoft Windows Hyper-V-Virtualisierungstechnologie dar. Auf Basis dieser Technologie werden die Fachanwendungen in verschiedenen, voneinander getrennten Netzwerkzonen mit unterschiedlichen Sicherheitsanforderungen betrieben. Eine Kopplung der verschiedenen Netzwerkzonen ohne Firewall-Trennung wird durch physische, technische und organisatorische Maßnahmen verhindert. Zudem unterbindet die physische Partitionierung der „Polizei-Cloud" einen gemeinsamen Betrieb von virtuellen IT-Systemen mit einem unterschiedlichen Sicherheitsbedarf auf einem Virtualisierungsserver.

Die virtuellen Systeme werden nun zentral in zwei Rechenzentren in Mainz, die mit den Computern der Polizei-Dienststellen verbunden sind, betrieben. Ein unbefugter Zugriff auf die Daten ist nicht möglich, da die Rechenzentren isoliert und gesichert vom LDI betrieben werden. Damit liegt die alleinige Verantwortung der Datensicherheit beim LDI.

Reduzierung von Aufwand und Kosten

Die mit Unterstützung von Avanade implementierte Private-Cloud-Lösung unterstützt den LDI dabei, schnell und einfach neue Systeme zu provisionieren und zu verwalten sowie diese vor unbefugtem Zugriff gemäß höchster Sicherheitsanforderungen zu schützen. Dank der nahtlosen Integration der System-Center-Produkte mittels Opalis konnte der Betriebsaufwand signifikant reduziert werden. Die dadurch freigewordenen Kapazitäten lassen sich in neue Projekte und Innovationen investieren. Des Weiteren wurde die Zahl der Server im Landesbetrieb Daten und Information um 34 Prozent gesenkt und damit auch die jährlichen Strom- sowie Lizenzkosten. Davon profitieren nicht nur die Kunden des LDI, wie die Polizei des Landes Rheinland-Pfalz, sondern auch die Mitarbeiter. ■

Matthias Bongarth,
Geschäftsführer
Landesbetrieb Daten und Information

Karsten Lutter,
Director Consulting
Avanade Deutschland GmbH

maxIT und GfWI – zwei Partner, eine Lösung für den Mittelstand

Sichere Services in der Cloud

Gemeinsam bieten die beiden Microsoft-Partner maxIT und GfWI mittelständischen Unternehmen ein umfassendes Leistungsportfolio für Microsoft Business-Lösungen aus der Cloud. Mittelständische Unternehmen profitieren dabei von der gebündelten Kompetenz der beiden Partner, einer schnellen und effizienten Projektumsetzung sowie einer sicheren und leistungsstarken Infrastruktur, die alle Compliance-Anforderungen erfüllt.

Cloud Computing bietet gerade für mittelständische Unternehmen große Chancen. Der Aufwand für die Inhouse-Betreuung der IT-Infrastruktur sinkt, ebenso wie die Aufwendungen für Investitionen in Hard- und Software. Zudem können Unternehmen stets die aktuellste und modernste Software nutzen und die Kosten sind – dank monatlicher Abrechnung – transparent. Dennoch haben viele mittelständische Unternehmen Bedenken, ihnen fehlt das Vertrauen – weniger in die Technologie als in die Informationssicherheit, die Rechtskonformität und den Datenschutz.

Mit diesen Bedenken sah sich auch die GfWI, die Gesellschaft für Wirtschaftsinformatik mbH, konfrontiert. Das mittelständische Software- und Beratungshaus vertreibt und implementiert Unternehmenslösungen auf der Basis von Microsoft-Technologien. Neben Integration und Implementierung bietet das Unternehmen auch weitere Services wie Lösungsentwicklung und Anpassungen an individuelle Anforderungen sowie Schulung und Support. Basis des Lösungsportfolios ist Microsoft Dynamics™ CRM. Die GfWI ist Microsoft Gold Certified Partner und wurde 2012 in den Microsoft President's Club aufgenommen.

Um das eigene Leistungsportfolio zu erweitern und neuen wie auch bestehenden Unternehmen Cloud-Services anbieten zu können, suchte die GfWI einen kompetenten Partner. „Professionalität in der Zusammenarbeit und der Betreuung der Kunden, Datenschutz und Informationssicherheit sowie eine moderne, hochverfügbare Infrastruktur – das waren die Anforderungen, die wir an eine partnerschaftliche Kooperation mit einem Managed Cloud Provider stellten", erklärt Joachim Stein, Geschäftsführer der Gesellschaft für Wirtschaftsinformatik mbH.

maxIT – maximale Verfügbarkeit, maximale Flexibilität

In der maxIT Consulting GmbH fand die GfWI einen Partner, der sich ebenfalls auf mittelständische Unternehmen fokussiert und die Ansprüche des Software- und Beratungshauses – sowohl an die technische Infrastruktur als auch an die Sicherheit, Rechtskonformität und den Datenschutz – erfüllen kann. Das Unternehmen betreibt in einem hochverfügbaren Rechenzentrum die Managed Cloud Services für Microsoft-Lösungen sowie auch individuelle Kundenanwendungen. Zum Microsoft-Portfolio gehören Hosted Dynamics CRM, Hostend Dynamics NAV, Hosted SharePoint, Hosted Exchange und Hosted Lync. „Unternehmen, die mit GfWI und maxIT zusammenarbeiten, können sich ihr gewünschtes Lösungsportfolio individuell und flexibel zusammenstellen. Wir bieten ihnen eine Plattform an, auf der sie alle ihre Geschäftsprozesse optimal abbilden können. Sie werden von uns umfassend beraten, haben ihren individuellen Ansprechpartner und können sich unser Rechenzentrum auch ansehen", ergänzt Marc-Sebastian Marggraf, Geschäftsführer der maxIT Consulting GmbH.

Für Sicherheit ist gesorgt

Die maxIT bietet in ihrem Rechenzentrum eine garantierte Verfügbarkeit von 99 Prozent. Das Service-Team des Unternehmens betreut die Kunden rund um die Uhr – 24 Stunden am Tag, 365 Tage im Jahr. maxIT betreibt die IT-Infrastruktur ausschließlich in Deutschland. Damit unterliegen alle personenbezogenen Daten sowie alle Geschäftsdaten dem deutschen Bundesdatenschutzgesetz, und die Rechtslage

„Die Flexibilität, die umfassende und kontinuierliche Betreuung und der sichere Rechenzentrumsbetrieb in Deutschland sind für mittelständische Unternehmen bedeutende Kriterien, um sich für Cloud Computing zu entscheiden."

Marc-Sebastian Marggraf
Geschäftsführer maxIT Consulting GmbH

ist stets eindeutig. Kunden profitieren von einem Höchstmaß an Sicherheit, und die Vertraulichkeit der Daten ist zu jedem Zeitpunkt gewährleistet. „Unserer Erfahrung nach sinkt die Skepsis mittelständischer Unternehmen, wenn gewährleistet ist, dass die Data Center in Deutschland betrieben werden und auch ihre Geschäftsdaten in Deutschland bleiben", ergänzt Marc-Sebastian Marggraf von maxIT.

Das Rechenzentrum von maxIT ist darüber hinaus nach dem national wie international anerkannten Standard ISO 27001 zertifiziert. Dies bedeutet, dass maxIT ein effektives Sicherheits- und Risiko-Management-System implementiert hat, um die Daten der Kunden zu schützen. Die maxIT setzt in ihrem Rechenzentrum in Deutschland zudem modernste Sicherheitstechnologien und -produkte ein. Ein durchgängiges Identity Management über alle Systeme und Anwendungen hinweg sorgt dafür, dass alle Identitäten, Benutzerprofile und Zugriffsberechtigungen sicher und konsistent verwaltet werden.

Weitere Informationen finden Sie auf den Websites der maxIT Consulting GmbH (www.maxit-consulting.de) und der GfWI, der Gesellschaft für Wirtschaftsinformatik mbH (www.gfwi.de).

GfWI & maxIT – schnell, effizient, sicher

Dank der Zusammenarbeit der beiden Unternehmen GfWI und maxIT profitieren mittelständische Unternehmen von der kompetenten Beratung, Betreuung und Lösungsumsetzung aus einer Hand – sei es für Lösungen on premise oder auch aus der Cloud. „Klar definierte Prozesse, eine schnelle und reibungslose Zusammenarbeit, Lösungskompetenz und ein hohes Verantwortungsbewusstsein gegenüber unseren Kunden kennzeichnen die Zusammenarbeit unser beider Unternehmen", erklärt Marc-Sebastian Marggraf von maxIT. „Mittelständische Unternehmen finden in uns einen Partner auf Augenhöhe." Entscheidet sich ein Kunde für die Zusammenarbeit mit GfWI und maxIT, wird in partnerschaftlicher Zusammenarbeit ein Lösungskonzept für die Einführung und Nutzung der Microsoft-Standard-Software erarbeitet. Die GfWI setzt hierbei oftmals auf die im eigenen Hause definierte Projektvorgehensweise „BlitzStart", die aus zwei Stufen besteht. In der ersten Stufe werden die Anforderungen, die aus den Geschäftsprozessen entstehen, definiert, die Standard-Software wird individuell angepasst und mit den „GfWI BlitzStart Tools" (Vorkonfiguration, Einrichtungsassistenten, Datenimport etc.) in Betrieb genommen. In der Zusammenarbeit mit maxIT fungiert die GfWI als primärer Ansprechpartner und übergibt die Lösung in das Rechenzentrum des Managed Cloud Provider. Damit ist die GfWI in der Lage, innerhalb von vier Stunden eine voll funktionierende Business-Lösung auf Basis von Microsoft-Technologien bereitzustellen. Die GfWI kann darüber hinaus das von maxIT bereitgestellte Selbstverwaltungsportal nutzen, beispielsweise für die Benutzerverwaltung, und hat damit vollen Zugriff auf die Lösung des Kunden. Die Stufe 2 der Projektmethode „BlitzStart" erfolgt nach der Inbetriebnahme der Lösung. Hier werden dann – falls notwendig – noch Änderungen und Anpassungen vorgenommen. ■

Julia Balzer,
Assistenz der Geschäftsführung
maxIT Consulting GmbH

The Wise IT-Guys

Als unabhängiges Beratungsunternehmen und Microsoft Gold-Partner in Deutschland unterstützt die SecuLink GmbH Unternehmen dabei, auf Basis modernster Technologien eine zuverlässige, sichere und kosteneffiziente IT-Infrastrukturen aufzusetzen, Geschäftsprozesse optimal zu gestalten und größtmögliche Zukunftssicherheit zu schaffen.

Entdecken Sie den Mehrwert professioneller IT-Services

Als Microsoft Software Asset Management Partner begleitet Sie SecuLink dabei, den Softwarebestand Ihres Unternehmens in allen Phasen des Lebenszyklus zu verwalten, zu kontrollieren und zu schützen.

Unsere Leistungen:

- Lizenzevaluierung und Abgleich der erworbenen mit den installierten Lizenzen
- SAM-Optimierungseinstufung und Optimierung Ihres bisherigen Software Asset Managements
- Microsoft SAM-Zertifikat (jährlich)
- Erstellung von Lizenzbilanzen durch SAM-Consultants

Gehen Sie auf Nummer sicher – mit einem zuverlässigen Partner

Als Microsoft IT-Security Gold Partner verfügt SecuLink über langjährige Erfahrung im Bereich IT-Sicherheit und berät Unternehmen bei der Auswahl der optimalen Security-Lösung – kompetent und unabhängig.

Unsere Leistungen:

- Kundenindividuelle Sicherheitskonzepte
- Sicherheitsanalyse und Risikoanalyse
- Realisierung von IT-Security-Lösungen mit namhaften Firewall-Produkten
- Incident Response & Notfallplanung
- Penetrationstest
- Risiko-Management

The Wise IT-Guys
SecuLink

Kontaktieren Sie uns:
SecuLink GmbH
Arndtstraße 21/2
71229 Leonberg
Tel. +49 (0)7152 948110
Fax +49 (0)7152 7647581
E-Mail: info@seculink.de
www.seculink.de

Microsoft Partner

Silver Messaging
Silver Hosting
Silver Volume Licensing
Silver Software Asset Management
Silver Midmarket Solution Provider

Hochverfügbarkeit aus dem Rechenzentrum von ACP

Mehr Flexibilität und Effizienz durch Datenauslagerung

Das Beratungsunternehmen Engel & Zimmermann wächst kontinuierlich und trägt für die sensiblen Daten seiner Kunden eine hohe Verantwortung. Grund genug, um die interne IT-Infrastruktur durch einen Cloud-Service in einem externen Data Center abzusichern. In ACP fand das Unternehmen den passenden Partner.

Die 1986 gegründete Engel & Zimmermann AG ist eine inhabergeführte Unternehmensberatung und gehört zu den führenden deutschen Beratungs- und Dienstleistungsunternehmen auf dem Feld der Wirtschafts-, Finanz-, Krisen- und Markenkommunikation. Das Dienstleistungsspektrum geht weit über das einer reinen PR-Agentur hinaus und reicht von der Betreuung der Wirtschafts-, Publikums- und Fachpresse über die Kommunikation des Going Public (IPO) bis hin zu Publikationen, interner Kommunikation und Online-PR. Zusätzlich werden Medien- und Auftrittstrainings sowie die Konzeption und Erstellung professioneller Bewegtbilder angeboten. Die besonderen Stärken liegen in der individuellen, auf den Kunden zugeschnittenen Dienstleistung und strategischen Beratung. Engel & Zimmermann arbeitet für Unternehmen mit unterschiedlicher Branchenausrichtung. Ein Schwerpunkt liegt auf der Betreuung von mittelständischen Firmen aus den Bereichen Investitionsgüter, Lebensmittel, Handel und Dienstleistungen, Konsumgüter und Marken sowie Gesundheit.

Verfügbarkeit hat höchste Priorität

Engel & Zimmermann gilt als eine der erfolgreichsten Kommunikationsagenturen in Deutschland mit einem namhaften Kundenkreis. Hohe Verfügbarkeit und Kompetenz – gerade in Krisensituationen – zeichnen die Agentur aus. Bisher wurden alle Kundendaten inhouse verwaltet.

Aufgrund des enormen Wachstums und der ständig steigenden Verantwortung bei der Datensicherung hat sich das Beratungsunternehmen entschieden, die ACP-Lösung „Infrastructure as a Service" (IaaS) aus dem ACP-Rechenzentrum zu beziehen und seine Daten zukünftig im Rechenzentrum vorrätig zu halten. „Damit können wir sicherstellen, dass alle Daten absolut sicher abgelegt und immer für unsere Kunden verfügbar sind. Das zeichnet uns aus und wird von unseren Kunden auch so erwartet", erklärt Frank Schroedter, Vorstand bei Engel & Zimmermann.

Dabei sorgt ACP dafür, dass zwischen dem Data Center des Kunden und dem ACP Data Center oder aber auch nur per Internet-Connect eine hochverfügbare Desktop-Plattform mit allen nötigen Anwendungen performant bereitgestellt wird. „Dadurch konnte eine wesentlich höhere Verfügbarkeit und Performance geliefert werden, als dies on premise mit dem gleichen Budget möglich gewesen wäre", erklärt Benedikt Fischer, Leitung Business Development ACP Cloud Computing. Die Hardware des Kunden wurde durch ein hybrides Konstrukt aus on premise und RZ-Komponenten im Bereich „Infrastructure as a Service" umgesetzt. Die aufgrund des Alters zu ersetzenden Geräte und Server wurden durch ein hochflexibles und ausfallsicheres Konstrukt aus dem ACP-Rechenzentrum erneuert.

Hochflexibel und effizient

Die Technik basiert auf dem ACP Virtual Datacenter. Backup, Firewall und Desaster Recovery sind somit Teil der Gesamtlösung. Snapshots, die im virtuellen Umfeld direkt als duplizierte und komprimierte Daten ins Backup-RZ der ACP geliefert werden, erhöhen die Verfügbarkeit zusätzlich. Das Gesamtprojekt beinhaltet aus allen Bereichen von On-premise-Hardware und -Software bis SaaS (Exchange-Mailboxen von Microsoft) die gesamte Produktpalette der ACP Cloud Dienste.

Für Engel & Zimmermann ergeben sich nun klare Vorteile. Zum einen entstand ein enormer Effizienzgewinn: „Bei Infrastructure as a Service im klassischen Modell werden meistens Hardware und Software-Stack komplett aufgebaut und verursachen so einen sehr hohen Ressourceneinsatz im Betrieb und bei der Wartung. Die Sharingeffekte fehlen dabei. Im ACP-Modell wird dies im ACP-RZ übernommen, sodass keine Overhead-Kosten durch zukünftige Erweiterungen entstehen und damit die Effizienz steigt", hält Benedikt Fischer fest. Zum anderen hat der Kunde mehr Flexibilität. Beim ACP IaaS werden der benötigte Speicherplatz sowie eventuell nötige Computing-Ressourcen sehr flexibel vorgehalten. Dies ist jederzeit erweiterbar. Dazu Frank Schroeter: „Wir können unser weiteres Wachstum problemlos vorantreiben und unsere Kunden jeder Zeit und in jeder Situation bestens betreuen – das ist für uns entscheidend!" ■

Peter Zach,
Vorstand der ACP IT Solutions AG

Dr. MORAWIETZ GmbH
CONSULTING • DEVELOPMENT • IT-SERVICES

SCHRITT FÜR SCHRITT ZU COMPLIANCE-KONFORMITÄT

WIE SICHER IST IHR DATEISYSTEM? MACHEN SIE DEN CHECK!

Nirgends sieht man die Probleme einer gewachsenen Struktur deutlicher als beim Umgang der Datenablage auf zentralen Fileservern. Undurchsichtige Berechtigungsstrukturen, vergessene Zugriffsrechte längst ausgeschiedener Mitarbeiter, kein Vier-Augen-Prinzip bei der Vergabe von Rechten, fehlende Kontrollmechanismen – all dies birgt erhebliche Risiken für die Datensicherheit und verletzt die grundlegenden Anforderungen von Risikomanagement und Compliance.
Der Dr. MORAWIETZ Experten-Check erfasst und analysiert die Berechtigungen und Schwachstellen in Windows-Dateisystemen. Management sowie Risiko- und Sicherheitsverantwortliche bekommen eine zuverlässige Beurteilung der Qualität und IT-Compliance beim Thema Zugriffssicherheit.

BERECHTIGUNGSANALYSE:
WER DARF WAS?

Standard-Reports geben detailliert Auskünfte:
- Welche Benutzer sind im untersuchten Bereich berechtigt?
- Welche Gruppen sind dort berechtigt?
- Worauf ist ein bestimmter Benutzer wie berechtigt?
- Aus welchen Gruppen stammen die Rechte?
- Welche Benutzer sind auf einem bestimmten Ordner wie berechtigt?
- Welche Benutzer sind die Besitzer der Ordner?
- Welche Shares gibt es? Sind sie verschachtelt?
- Wird mit Deny-Berechtigungen gearbeitet?
- Wo sind verwaiste Benutzerkonten berechtigt?

Und andere mehr

SICHERHEITSANALYSE:
WO SIND RISIKEN?

Risiko-Indikatoren zeigen:
- Wo bestehen konkrete Sicherheitsprobleme?
- Wo werden Compliance-Richtlinien verletzt?

ERGEBNISBERICHT:
WAS TUN?

Konkrete Handlungsempfehlungen und Beratung:
- Welches sind die dringendsten Aufgaben?
- Wie könnte ein standardisiertes Dateisystem-Konzept aussehen?

UNSER ANGEBOT FÜR SIE:
- Tool-gestütztes Auslesen der effektiven Rechte aus Ihrem Dateisystem
- Analyse und Aufbereitung der Informationen in „lesbaren" Reports
- Bewertung und Präsentation der Ergebnisse mit konkreter Beratung

die volle Leistung ab 3.900 Euro!*
* Maximal zwei Tage Datenscan vor Ort; Preis zzgl. Reisekosten und MwSt.

Mehr erfahren Sie unter www.morawietz.com/compliance

Microsoft Partner
Silver Server Platform
Silver Identity and Access
Silver Software Asset Management
Silver Midmarket Solution Provider

Dr. MORAWIETZ
Consulting & Training GmbH
Schwanheimer Straße 144a
64625 Bensheim
Telefon +49 (6251) 10 58-0
Telefax +49 (6251) 10 58 10
E-Mail Info@MORAWIETZ.de
Internet www.morawietz.com

Im Überblick

Microsoft-Partner in diesem Kompendium:

Partner	Internet	Seite
ACP IT Solutions AG	www.acp.de	65
Alegri International Service GmbH	www.alegri.eu	27
AMPEG GmbH	www.ampeg.de	56
Ashampoo GmbH & Co. KG	www.ashampoo.com	46
Avanade Deutschland GmbH	www.avanade.com	61
COMPAREX AG	www.comparex.de	38
CWD-Solution GmbH	www.cwd-solution.com	36
GWAVA EMEA GmbH	www.gwava.eu	20
HSBD GmbH	www.apde-org.eu	22
infoWAN Datenkommunikation GmbH	www.infowan.de	58
iTernity GmbH	www.iternity.com	42
Materna GmbH	www.materna.de	50
maxIT Consulting GmbH	www.maxit-con.de	62
MERENTIS Consult GmbH	www.merentis.com	54
Dr. MORAWIETZ Consulting & Training GmbH	www.morawietz.de	31
Net at Work Netzwerksysteme GmbH	www.netatwork.de	40
Omada GmbH	www.omada.net	44
Oxford Computer Group GmbH	www.oxfordcomputergroup.de	24
PRW Rechtsanwälte	www.prw.de	22
SecuLink GmbH	www.seculink.de	64
SFC Software for Companies GmbH	www.sfc-software.de	33
T-Systems International GmbH	www.t-systems.de	52
unique projects GmbH & Co. KG	www.unique-projects.com	09
WMC GmbH	www.wmc-direkt.de	29
WTS Group AG	www.wts.de	18

Windows Azure

Datenschutz und Compliance nach den neuesten Standards.

Windows Azure ist die Cloud-Plattform von Microsoft, die Sicherheit und Datenschutz nach EU-Norm gewährleistet sowie Compliance-Vorgaben erfüllt. So können Sie sich voll und ganz auf das konzentrieren, was wirklich zählt: Ihre Anwendungen und deren Mehrwert für Ihre Kunden und Benutzer.

Jetzt informieren unter **aka.ms/vertrauenscenter**

Microsoft

IT-Compliance &
IT-Governance

Produkte &
Technologien

Security &
Cloud Computing

www.microsoft.de/it-business-network

Informations-Sicherheit

Microsoft

Microsoft Deutschland GmbH
Konrad-Zuse-Straße 1
85716 Unterschleißheim
Tel. +49 (0)89 31 76-0
Fax +49 (0)89 31 76-1000
www.Microsoft.com