Sicherheits-Leitfaden

Risikominimierung durch mehr Datensicherheit

Das Thema Informationssicherheit im Unternehmen existiert nicht erst seit gestern, aber die Nutzung von IT-Systemen, digitalen Kommunikations- und Vertriebskanälen sowie das Internet haben bei der Art, wie wir diese Aufgabe angehen, einen Paradigmenwechsel ausgelöst. Bedenkt man dann noch, mit welch rasantem Tempo sich die Technologien weiterentwickeln, müsste eigentlich jeder für die Informationssicherheit Verantwortliche Sisyphos als zweiten Vornamen tragen.

Was die Sache weiter kompliziert, ist die Tatsache, dass „der Feind“ in der Regel im Büro nebenan sitzt.

So stellt sich die Frage welche Möglichkeiten bestehen, um mit weniger Aufwand und Bauchweh für mehr Informationssicherheit zu sorgen. Mehr dazu auf den folgenden Seiten.

Inhalt

1 Thema Informationssicherheit – Wolke mit Silberrand?

Das Thema Informationssicherheit im Unternehmen existiert nicht erst seit gestern; denn auch in den Zeiten ordnerstarrender, papierbasierter Ablagen war es natürlich von größter Bedeutung, wichtige Firmendaten sicher verwahrt zu wissen. An der Aufgabenstellung an sich hat sich seitdem zwar nichts geändert, aber die mittlerweile übliche Nutzung von IT-Systemen, digitalen Kommunikations- und Vertriebskanälen sowie das Aufkommen des Internet haben bei der Art, wie wir diese Aufgabe angehen, dennoch einen Paradigmenwechsel ausgelöst.

Reichte es Anfang der Achtzigerjahre noch aus, wichtige Firmendaten abends im Tresor einzuschließen und auf die Arbeitsmoral des Nachtwächters zu vertrauen, sehen sich Management und IT-Verantwortliche heute mit einer Vielzahl von Aufgaben und Anforderungen konfrontiert, um unternehmensweit bestmögliche Informationssicherheit zu gewährleisten.

So gilt es, personenbezogene und allgemeine Firmendaten vor Missbrauch zu schützen, bei der Nutzung und Übertragung von Daten Vertraulichkeit sicherzustellen sowie absolute Datenintegrität und-authentizität zu gewährleisten, und das bei einer möglichst nahtlosen Datenverfügbarkeit. Dabei ist der Übergang zum Thema IT-Sicherheit durchaus fließend. Denn um Informationssicherheit überhaupt erst bieten zu können, müssen Hardware und Software einwandfrei funktionieren und mit entsprechenden Sicherheitstechniken wie Virenscannern, Firewalls und Systemen für das Zugriffsmanagement ausgestattet sein. Dass man seine Systeme und Daten bei all diesen Bedrohungen auch gegen eher „altmodische“ Risiken absichern sollte, wie Blitzschlag, Feuer, Wasserschäden, technische Defekte oder Diebstahl, dürfte sich von selbst verstehen.

2 Der Paragrafendschungel wird immer dichter

Das Thema Business Continuity, also die möglichst nahtlose Weiterführung des Geschäftsbetriebs nach Störfällen, und die hierfür erforderlichen Maßnahmen und Systeme klammern wir an dieser Stelle einfach mal aus, um die Dinge nicht noch weiter zu komplizieren. Dafür sorgen schon Gesetzgeber, Regulierungsbehörden und Verbände, die Unternehmen immer stärker in die Pflicht nehmen und mit Gesetzen, Verordnungen, Governance-Standards und Compliance-Bestimmungen ein nur schwer überschaubares Regelwerk schaffen, dessen Nichtbeachtung für die Verantwortlichen durchaus zivil- oder gar strafrechtliche Konsequenzen nach sich ziehen kann. So ist man heute gut beraten, jemanden an Bord zu haben, der sich mit dem Bundesdatenschutzgesetz (BDSG) und der Datenschutzrichtlinie 95/46/EG ebenso auskennt wie mit dem Telekommunikationsgesetz (TKG), der Richtlinie 2002/58/EG und Compliance-Anforderungen wie dem Sarbanes-Oxley Act (SOX) und dem Federal Information Security Management Act (FISMA).

Auch die distribuierte Verarbeitung von Daten stellt die Unternehmen zunehmend vor Probleme, vor allem dann, wenn in solche Strukturen involvierte Dienstleister in Ländern beheimatet sind, deren Datenschutzgesetze den EU-Standards nicht entsprechen.

3 Offene Flanken wohin man schaut

Wie komplex und überaus anspruchsvoll das Thema Informationssicherheit mittlerweile geworden ist, zeigt sich vor allem an einem aktuellen globalen IT-Hype: BYOD. Dieses Akronym steht für „Bring your own device“ und bezeichnet den Trend, nicht nur mobil auf Unternehmensnetzwerke und Applikationen zuzugreifen, sondern dazu in zunehmendem Maße auch eigene Hardware zu nutzen, seien es Smartphones, Tablets oder Notebooks. Eine weltweite Umfrage von PricewaterhouseCoopers[1] unter CIOs von Januar 2012 ergab, dass 28 % ihrer Mitarbeiter für berufsbezogene Aufgaben Privatgeräte nutzten. Die Prognose für Mitte 2013 lag da bereits bei 35 %. Wenn man bedenkt, dass Mitarbeiter, Partner und Lieferanten mit den unterschiedlichsten Gerätetypen, Marken und Betriebssystemen auf die Unternehmensinfrastruktur zugreifen, wird schnell klar, wie schwierig es ist, einer solchen heterogenen Gerätebasis mit einer einheitlichen Sicherheitslösung entgegenzutreten.

Gewiss könnte man das Sicherheitsproblem mindern, indem man lediglich unkritische Daten und Anwendungen für den mobilen Zugriff freigibt, dabei stellt sich aber stets die Frage, inwiefern das die Effizienz und Produktivität des Unternehmens ausbremst.

Zudem sprechen wir nicht von nur einem Zugangspunkt zum Herzen des Unternehmens, der ähnlich wie ein Grenzübergang, mit relativ überschaubarem Aufwand gesichert werden könnte, sondern von multiplen Zugriffsmöglichkeiten. So gilt es nicht nur, Kunden- und Produktdatenbanken, Preislisten und das Online-Bestellsystem zu schützen, sondern auch Finanzdaten und -anwendungen, Forschungs- und Entwicklungsdaten, Marketingpläne, offene Tools wie Notes oder SharePoint und das geistige Eigentum des Unternehmens – von profanen Dingen wie Telefon, E-Mail und Instant Messaging mal ganz zu schweigen. Bedenkt man dann noch, mit welch rasantem Tempo sich in nahezu allen IT- und Kommunikationsbereichen die Technologien weiterentwickeln, müsste eigentlich jeder für die Informationssicherheit Verantwortliche Sisyphos als zweiten Vornamen tragen.

Was die Sache weiter kompliziert, ist die Tatsache, dass „der Feind“ nicht irgendwo im Verborgenen lauert, sondern in der Regel im Büro nebenan sitzt. Ganz gleich, welche Studie zum Thema Informationssicherheit man bemüht, alle kommen sie zu dem Schluss, dass interne Hacker, nicht autorisierte Benutzer, das eigenmächtige Verändern der PC-Sicherheitseinstel-

lungen, die Nutzung unerlaubter Anwendungen, ungeschützte Hardware und der Verlust mobiler Speichermedien für den Großteil aller Sicherheitsprobleme verantwortlich sind.

In diesem Bereich vorbeugend tätig zu werden, birgt allerdings die Gefahr, dass die Mitarbeiter sich bespitzelt und überwacht vorkommen, was erst recht Fronten schafft und den Teamgeist untergräbt. So gilt es hier, mit größtmöglichem Fingerspitzengefühl vorzugehen.

Das soll aber nicht heißen, dass man all den Gefahren, die draußen in den Weiten des Web sowie in der realen Welt lauern, nur am Rande Beachtung schenken muss. Ganz im Gegenteil, denn Viren, Trojaner und Würmer sind für Unternehmenssysteme ebenso reale Bedrohungen wie Spoofing, Pharming, Phishing oder Denial of Service-Angriffe, um nur einige zu nennen. Das Hacker-Business hat dabei in den letzten Jahren einen enormen Professionalisierungsschub erlebt. Wie jede Branche setzen auch die Cyberkriminellen zunehmend auf automatisierte Abläufe, die einfach skalierbare Strukturen ermöglichen, was wiederum die Gewinne steigert. War das Hacken noch vor wenigen Jahren ein Multimilliarden-Dollar-Business, schätzt man heute die in der Branche weltweit erzielten Umsätze auf über eine Billion Dollar. Betrachtet man diese Dynamik und Größenordnungen wird schnell klar, dass die Gewährleistung von Informationssicherheit allenfalls ein reaktives Unterfangen ist, bei dem es vor allem darum geht, mit der Innovationskraft und dem Tempo der Hacker-Branche Schritt zu halten.

Da sich an dieser Situation voraussichtlich auch mittelfristig nichts ändern wird, sind neue Ansätze gefragt, mit denen sich die Informationsläufe beschleunigen lassen. Wir leben in den Zeiten der sozialen Medien und der weltweiten Vernetzung und die Wirtschaft wäre gut beraten, diese Kommunikationsstrukturen zu nutzen, um durch eine engere Verzahnung zumindest in Teilbereichen wieder schneller zu werden und der Hacker-Szene mit pro-aktiven Maßnahmen begegnen zu können.

Info:

Spoofing: Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.

Phishing: Versuche, über Web-Seiten oder E-Mails an Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

Pharming: Eine Weiterentwicklung des klassischen Phishings, manipuliert die DNS-Anfragen (Domain Name System) von Webbrowsern durch Trojaner und Viren, um den Benutzer auf gefälschte Webseiten umzuleiten.

Denial of Service: Ist die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. Kann durch unbeabsichtigte Überlastungen verursacht werden, oder durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten im Datennetz.

„Mobil auf Unternehmensnetzwerke und Applikationen zugreifen mit Smartphones, Tablets oder Notebooks – durch CRM Cloud auf der höchsten Sicherheitsstufe. “

4

Mehr Informationssicherheit durch die Cloud

Aber betrachten wir die Dinge einfach mal von der anderen Seite und stellen die Frage, welche Möglichkeiten bestehen, um diese Mammutaufgabe mit weniger Aufwand und Bauchweh zu stemmen und dabei für mehr Informationssicherheit zu sorgen. Was bei genauer Betrachtung der Schwachstellen und Risikobereiche auffällt ist, dass viele davon mit dem zusammenhängen, was man mittlerweile als „traditionelle" IT-Infrastruktur bezeichnet, also vor Ort installierten Servern, PCs und Speicherlösungen sowie der lokalen Applikations-Bereitstellung.

Die Logik dahinter ist denkbar einfach und zudem überaus schlüssig: Was nicht physisch vor Ort präsent ist, das kann auch nicht gestohlen, beschädigt oder manipuliert werden. Heißt das wiederum, man sollte herkömmliche IT-Modelle ein für allemal hinter sich lassen und sich nun schnellstmöglich mit fliegenden Fahnen in Richtung Cloud aufmachen? Die Antwort darauf ist ein klares „Ja gewiss, aber …".

Natürlich, Cloud-Computing bietet ein hohes Maß an Informationssicherheit und Datenschutz, ermöglicht bei optimaler Skalierbarkeit eine höhere Datenverfügbarkeit, macht unabhängig von eigenen Ressourcen und kann helfen, Kosten und Energieverbrauch zu senken.

Die Cloud-Vorteile auf einen Blick:

1. Schnelle, automatisierte Anwendungsbereitstellung
2. Flexibel skalierbare Lösung (Hinzufügen weiterer Nutzer)
3. Klare Vorteile bei Datenschutz und Informationssicherheit
4. Betrieb durch externen Dienstleister
5. Ortsunabhängiger Zugriff via Internet
6. Laufende Nutzungsgebühren statt Vorabinvestitionen
7. Weniger oder gar keine IT-Fachkräfte vor Ort nötig
8. Keine Hardware-Investitionen (Server)
9. Betrieb in abgesichertem Rechenzentrum

5
Eine solide Basis schaffen

Dennoch sind Cloud-Lösungen für die Unternehmen alles andere als ein Freibrief. So ändert die Cloud nichts an der unternehmerischen Verantwortung für die Daten und den Datenschutz. Dieser Aspekt ist umso wichtiger, als bei den Cloud-Services „Infrastructure as a Service“ (IaaS), „Platform as a Service“ (PaaS) und „Software as a Service“ (SaaS) in genau der Reihenfolge aufsteigend die Kontrolle über die eigenen Ressourcen in zunehmendem Maße beim Cloud Service Provider (CSP) liegt.

Das wiederum bedeutet, dass man bei der Auswahl des CSP genau hinschauen muss. Dabei sollte die angebotene Cloud-Architektur ebenso geprüft werden wie die Sicherheitskonzepte (Layered Defense) des Anbieters, die gebotenen Service-Level Agreements (SLA), die Audit-Qualität (wer beauftragt sie und wer ist der Auditor?), die physische Sicherheit der Cloud-Rechner und natürlich die wirtschaftliche Stabilität des CSP.

Außerdem sollte man bedenken, dass zahlreiche CSP in den USA ansässig sind, wo im Gegensatz zum EU-Raum Regierungsbehörden weitgehenden Einblick in die vorgehaltenen Daten verlangen können. In solchen Fällen (und nicht nur in solchen) empfiehlt sich ein Hybridkonzept, bei dem ein Teil der Daten in die Cloud verlagert wird, während alle datenschutzrelevanten Bereiche außerhalb verarbeitet werden.

Insgesamt lassen sich vier sicherheitsrelevante Ebenen identifizieren, die man vor Implementierung einer Cloud-Lösung gründlich durchleuchten sollte: CSP (Servicebereitstellung), Netzwerk (Transport und Speicherung von Daten), System (Zugriffskontrolle durch die Plattform) und Applikationen (Verarbeitung von Daten). Dabei kommt vor allem der Anwendungsebene eine besondere Bedeutung zu. Denn selbst die beste Cloud-Architektur ist nur so gut wie die Anwendungen, die man über sie fährt. Und auch hier gilt: Trau, schau wem. Bei der Partnerwahl sollte man hier vor allem auf folgende Punkte achten: Verfügt der Anbieter auch jenseits der Cloud über solide Erfahrung mit CRM- und ERP-Lösungen? Werden integrierte Komplettlösungen angeboten, die sich an die Anforderungen Ihres Unternehmens anpassen lassen? Sind attraktive Hosting- und Mietangebote im Portfolio? Gehören tägliche Backups und Updates zum Leistungsumfang?

Tipp

Sorgen Sie auf allen vier Ebenen für Sicherheit.

Cloud Service Provider
Verfügt der Anbieter über ein schlüssiges Layered Defense Konzept? Inwiefern ist er auditiert/zertifiziert? Ist er dem Safe Harbor Act beigetreten?

Netzwerk
Welche Verschlüsselungstechniken kommen zum Einsatz? Welche Sicherheits-Features werden bei der Datenspeicherung geboten? Existiert ein durchdachtes Business Continuity Konzept?

System
Wie einfach ist es, Anwender aufzunehmen und zu sperren? Welche Kontroll- und Sicherheits-Features gibt es für den mobilen Zugriff? Wie geht das System mit einer heterogenen Hardware-Basis (BYOD) um?

Applikationen
Sind die einzelnen Anwendungen für den Cloud-Einsatz optimiert? Wie stabil laufen sie? Gibt es Verfügbarkeitsprobleme? Werden individuell anpassbare Nutzungsmodelle angeboten?

Generell hat sich erwiesen, dass im traditionellen Umfeld seit langem etablierte Software-Häuser auch für Cloud-Strukturen meist besonders durchdachte und ausgereifte Lösungen zu bieten haben, da diese in der Regel auf den Funktionalitäten der bestehenden Produkte aufsetzen.

Sage CRM Cloud zum Beispiel ist eine gehostete Mietlösung, die ohne aufwändige IT-Infrastruktur auskommt. Zu einem festen monatlichen Preis bieten Ihnen Sage Cloud Lösungen ohne zusätzlichen Implementierungsaufwand alle Tools, die Sie für die Vermarktung und den Vertrieb benötigen – individuell anpasspar auf Ihre persönlichen Geschäftsprozesse. Gleichzeitig lassen sich damit die Kosten für Vertrieb, Marketing und Verwaltung reduzieren.

Die für ihre ausgereiften Funktionen in den Bereichen Warenwirtschaft und Rechnungswesen viel gelobte Sage Office Line zählt übrigens mittlerweile zu den weitverbreitetsten ERP-Systemen im Mittelstand.

Gerade für „Cloud-Anfänger“ sind solche gehosteten Komplettlösungen auf Mietbasis sehr zu empfehlen, da sie alle funktionalen Bereiche abdecken, keine Vorabinvestitionen erfordern und im laufenden Betrieb keine Kosten durch nicht benötigte Leistungsmodule anfallen. Außerdem lässt sich eine Mietlösung jederzeit flexibel an veränderte Anforderungen anpassen.

Zudem sollte man bei der Cloud-Software natürlich auch darauf achten, wie nahtlos sie sich in Ihre bestehende Infrastruktur integrieren lässt. Aber auch in dem Punkt hat sich gezeigt, dass die etablierten Anbieter Wert auf größtmögliche Kompatibilität gelegt haben.

Fazit

Geht man bei Partnerwahl und Migration umsichtig vor, lassen sich durch die Verlagerung von Aufgaben in die Cloud Vorteile erzielen: bei Produktivität, Kosten und Effizienz ebenso wie bei der Informationssicherheit. Natürlich ist die Cloud gerade bei letzterem Punkt kein Allheilmittel. Der zunehmende Übergang der Ressourcen-Kontrolle an den CSP birgt Risiken. Und es lassen sich bei einer Cloud-Lösung weitere kritische Bereiche identifizieren. Trotzdem sind die Schnittstellen zwischen CSP und Cloud-Nutzer überschaubar und klar definiert, so dass man hier mit wenigen Maßnahmen die Informationssicherheit optimieren kann. Zudem lassen sich in der Cloud gerade die internen Risiken deutlich reduzieren. Bedenkt man, dass nicht autorisierte Benutzer, Berechtigungsmissbrauch und Verlust von Speichermedien nach wie vor die mit Abstand größten Gefahren für die Informationssicherheit darstellen, wird deutlich, dass man gerade unter Sicherheitsaspekten an der Cloud heute nicht vorbei kommt und sie als echte Alternative zu traditionellen IT-Infrastrukturen einbeziehen sollte.

Internet: www.sage.de

Sage ist ein börsennotiertes Unternehmen der britischen Sage Gruppe, einem weltweit führenden Dienstleister für betriebswirtschaftliche Software für kleine und mittlere Unternehmen. Seit mehr als 25 Jahren wollen wir unseren Kunden das Plus an Freiheit geben, mit dem sie erfolgreich sein können. Sage weiß, dass jedes Unternehmen anders ist. Deshalb bieten wir Produkte und Services an, die unterschiedlichste Bedürfnisse abdecken, einfach und komfortabel zu bedienen und sicher und effizient sind. Sage hat über sechs Millionen Kunden und mehr als 13.500 Mitarbeiter in 24 Ländern: in Großbritannien und Irland, auf dem europäischen Festland, in Nordamerika, Südafrika, Australien, Asien und Brasilien. Mehr Informationen finden Sie unter www.sage.de

Sage Software GmbH | Emil-von-Behring-Straße 8-14 | 60439 Frankfurt am Main
Telefon: 069 50007-6111 | Fax: 069 50007-7208 | E-Mail: info@sage.de | www.sage.de
www.facebook.com/SageSoftwareGmbH

Technische, formale und druckgrafische Änderungen vorbehalten. Stand Juni 2013.