security@druckerei.de

Wie vertragen sich Datenbanken, CMS-Systeme und Cloud-Computing mit dem Thema IT-Sicherheit?

Keine Woche vergeht, ohne dass neue Cyberattacken bekannt werden. Verschiedene Staaten haben längst eigene Spezialeinheiten eingerichtet und sich damit im virtuellen Raum in Stellung gebracht. Und auch große Unternehmen investieren enorme Summen in die IT-Sicherheit, um die immer dreisteren Cyberattacken abzuwehren. Dass dies nicht so einfach ist, zeigen die jüngsten Beispiele, bei denen Hacker in die Netze von Sony und anderen Unternehmen, in die des US-Verteidigungsministeriums und in den Fahndungscomputer der deutschen Bundespolizei eingedrungen sind.
Dabei haben die Systeme eines gemeinsam: Sie zählen zu den sichersten der Welt. Wer diese Systeme knackt, kann auch alle anderen knacken. Doch viele andere Attacken werden durch die zunehmende Nutzung von Cloud-Computing, Smartphones und Tablets sowie Social-Media-Angeboten begünstigt.

Mangelndes Bewusstsein

Während sich große Unternehmen durchaus der Risiken aus dem Internet bewusst sind, fehlt gerade bei Klein- und Mittelbetrieben das Bewusstsein und auch eine klare Strategie im Umgang mit der drohenden Gefahr aus dem Internet. Hierbei stellt die Druckindustrie keine Ausnahme dar.
Einer der wichtigsten Rohstoffe und Schätze der Druckindustrie sind digitale Daten und gleichzeitig setzt sie wie kaum eine andere Branche in der Zusammenarbeit mit dem Kunden auf das Internet – ein Umstand, der Hackern im wahrsten Sinne des Wortes Tür und Tor auf die Server und Rechner der Druckereien öffnet. Zwar sind KMUs grundsätzlich nicht so häufig das Ziel von Hackern wie Großkonzerne, aber Viren, Trojaner, neugierige ›Script-Kiddies‹ und unzufriedene Mitarbeiter machen in dieser Hinsicht keinen Unterschied. Die Vorstellung, dass beispielsweise ein Geschäftsbericht, der auf den FTP-Server einer Druckerei hochgeladen wurde, schon vor der Veröffentlichung in die falschen Hände gerät, ist sicherlich das absolute Worst-Case-Szenario. Man muss aber nicht immer vom Schlimmsten ausgehen, es reicht schon, wenn ein Hacker in das MIS eindringt und dort Kundendaten, Angebote, Rechnungen und so weiter einsehen kann.

Schwachstelle Mensch

Technische Lösungen wie Virenscanner, Firewalls und Spamfilter gehören mittlerweile bei den meisten Unternehmen zur Standardausstat-

Das Thema IT-Sicherheit wird von Klein- und Mittelbetrieben vielfach unterschätzt. Eine der größten Schwachstellen stellt dabei der Mensch selbst dar.
Wir haben uns umgehört, wie sich Unternehmen der Druckindustrie dem Thema IT-Sicherheit stellen. Und wir geben Tipps, wie Sie sich gegen Angriffe von Hackern wappnen können.

Von Knud Wassermann

PASSWORTWAHNSINN

Kaum einer von uns ist heute noch in der Lage, sich alle Passwörter zu merken. Das Arbeiten im Internet erfordert aber laufend die Erstellung neuer Nutzer-Namen, die am Rechner abgespeichert werden – ein gefundenes Fressen für Hacker. Sie verwenden dazu Programme, die 250 Millionen Passwörter in der Sekunde knacken können. Verwenden Sie deshalb möglichst lange Passwörter mit mindestens zehn Zeichen. Dabei sollte jedes Zeichen nur einmal vorkommen. Verwenden Sie durchaus auch Sonderzeichen (wenn möglich) und meiden Sie die üblichen Namens- und Geburtstagskombinationen sowie lebende Sprachen. Ein weit verbreiteter Fehler ist die Verwendung von Universalpasswörtern (eines für alles) oder die automatische Speicherung der Passwörter im Webbrowser.

Tipp: Bilden Sie ganze Sätze und verwenden Sie die Anfangsbuchstaben für das Passwort.

Zum Beispiel:

Am 27. 10. gehen wir in die Kneipe am Markt = A2710gwidKaM.

Bei Software-Programmierern ist es seit Jahren ein geflügeltes Wort: »Der Teufel steckt in der Datei«. Doch inzwischen hat dieser Spruch seine Berechtigung vor allem, wenn es um IT-Sicherheit geht. Denn oft genug sind Viren oder Trojaner in einer Datei versteckt. 2006 hatte die Schweizer A&F Computersysteme AG diese Thematik in einer Anzeige in Szene gesetzt, in der dazu aufgefordert wurde, den Fehler-Teufel zur Hölle zu schicken.

tung, bei der Umsetzung von IT-Sicherheit in der Unternehmensorganisation gibt es aber noch große Defizite. Als große Schwachstelle macht hier eine Studie von IDC trotz aller Technik die Mitarbeiter aus.

Die Hälfte der im Rahmen der Studie befragten Unternehmen hat die Mitarbeiter als schwächstes Glied ihrer IT-Security-Kette genannt, gefolgt von Smartphones, Laptops und PC-Arbeitsplätzen. Die Studie empfiehlt Unternehmen, ihre Mitarbeiter zum Beispiel im Umgang mit E-Mails besser zu schulen. Zudem sollte die private Nutzung von E-Mails am Arbeitsplatz verboten werden.

Dies solle auch für die private Nutzung von Facebook und Twitter gelten. Angesichts der Bedeutung von Social Media in der Zielgruppe der 18- bis 40-Jährigen war es abzusehen, dass sich Hacker und Spammer die Verbreitung von Social Media zunutze machen würden. Nach den Beschäftigten wird vor allem die wachsende Zahl der Endgeräte als sicherheitskritisches Element der IT genannt, denn durch sie kann der Zugriff auf die Systeme und Unternehmensdaten quasi jederzeit und von überall aus erfolgen.

Die befragten Unternehmen sind zwar von der Qualität ihrer Schutzvorkehrungen und -einrichtungen überzeugt und stufen zu 60% den Schutz gegen Angriffe von außen als in hohem Maße sicher ein. Um den Sicherheitslevel zu halten, muss jedoch kontinuierlich in Technologie und Know-how investiert werden.

Sicherheit hat oberste Priorität

Beim Aurolzmünsterer Digitaldruckdienstleister Level2 hat man Erfahrung im Umgang mit sensiblen Kundendaten, weshalb das Thema IT-Sicherheit auch oberste Priorität hat. So wurde ein einbruchs- und vandalensicherer Serverraum geschaffen, die Daten werden in- und extern mehrfach gesichert. Gleichzeitig erfolgt die Zutrittskontrolle in den Sicherheitsbereich durch Schlüsselchips, und das Ganze wird rund um die Uhr per Video überwacht. »Wir verwalten für unsere Kunden sensible Daten und sorgen dafür, dass aus dem Sicherheitsbereich absolut nichts nach außen dringt«, versichert Geschäftsführer Alois Höller. Um den Sicherheitsgrad aufrechtzuerhalten, geht man bei Level2 sogar so weit, dass man in regelmäßigen Abständen Hackerangriffe von Profis simulieren lässt, um so die gesamte IT-Infrastruktur auf Herz und Nieren zu prüfen. Zusätzlich hat man für alle Mitarbeiter klare Verhaltensregeln im Umgang mit Daten aufgestellt und etwaige Sicherheitslücken wie etwa USB-Sticks und andere Wechselspeicher aus dem Unternehmen verbannt.

Klare Spielregeln für alle

Auch bei gugler cross media wird das Thema IT-Sicherheit sehr ernst genommen. Als Crossmedia-Dienstleister hostet das Unternehmen Hunderte von Websites und hat dazu eine starke IT-Abteilung aufgebaut, die sich auch um die Sicherheit der IT kümmert. Mit einer eigenen ▸

Checkliste

FRAGEN ZUR IT-SICHERHEIT

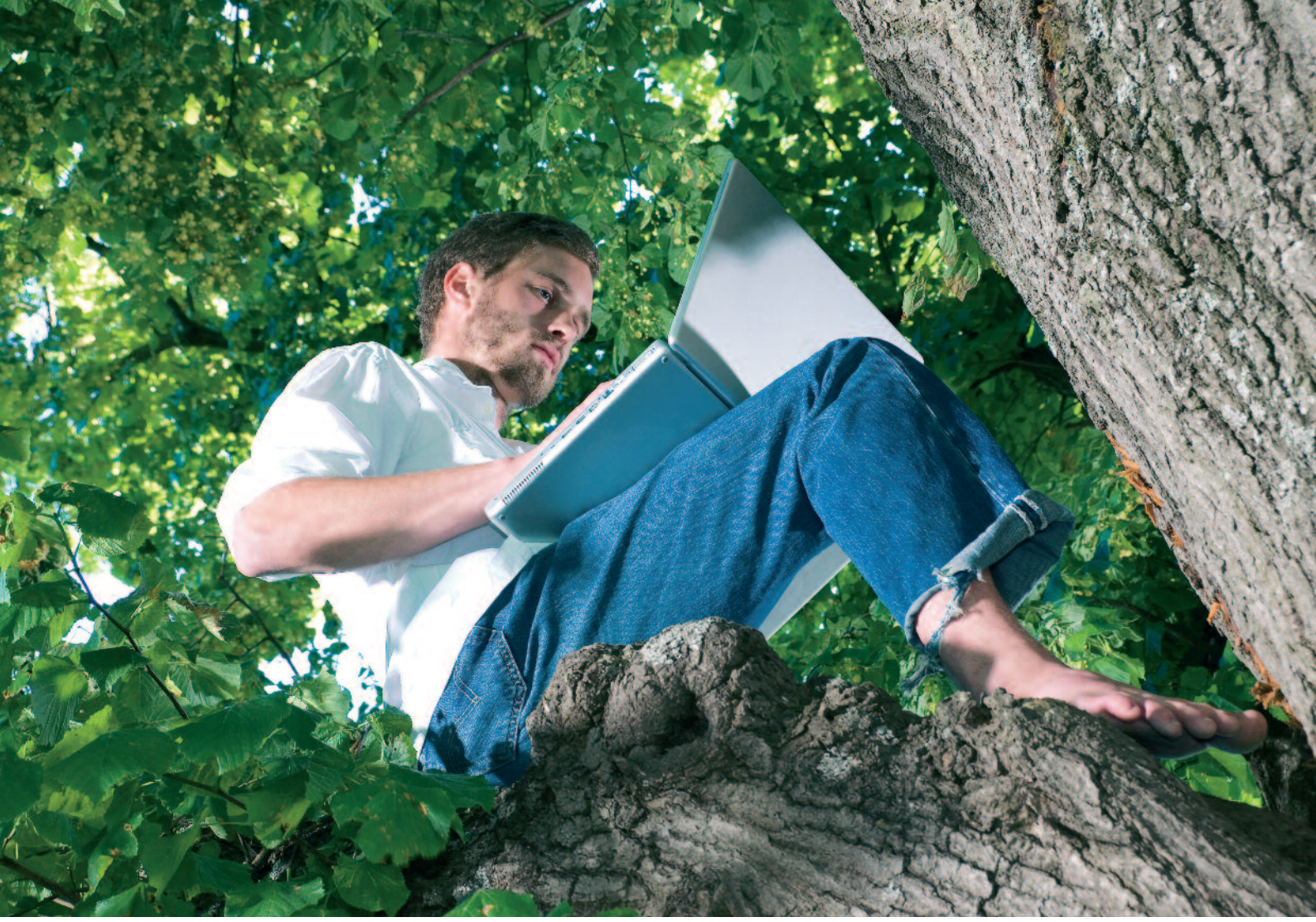
Bei mehr als jedem zweiten Unternehmen in Deutschland wird die IT-Sicherheit durch Zeitmangel beeinträchtigt. Häufig sind die Sicherheitsexperten im Tagesgeschäft mit Routinearbeiten ausgelastet. Die Einrichtung wichtiger Schutzmaßnahmen wie Beschränkungen des Zugriffs auf hochsensible Daten bleibt dabei auf der Strecke. Zu diesem Ergebnis kam eine Studie der Fachzeitschrift ›InformationWeek‹.
Die 10 Fragen zur IT-Sicherheit sollen daher ein wenig helfen, eine Sicherheitsstrategie zu entwickeln.

1. Ist die Verantwortung für die Datensicherheit eindeutig festgelegt? Wird diese mit der erforderlichen Sachkenntnis und Sorgfalt wahrgenommen?
2. Verfügt Ihr Unternehmen über klare schriftliche Anweisungen zum Gebrauch von Computern, Netzwerken, E-Mails und Internet und sind diese allen betroffenen Mitarbeitern nachweislich bekannt?
3. Wenn in Ihrem Unternehmen ein Netzwerk verwendet wird: Wissen Sie zuverlässig, dass es fachgerecht installiert wurde, und liegt die laufende Administration in entsprechend qualifizierten Händen?
4. Ist in Ihrem Unternehmen durch ein angemessenes Berechtigungssystem sichergestellt, dass die Installation von Programmen nur von fachkundigen Administratoren vorgenommen werden darf und kann?
5. Haben Sie umfassende Datensicherungs- und Notfallskonzepte und werden diese in regelmäßigen Abständen (zumindest einmal jährlich) einem Test unterzogen?
6. Ist sichergestellt, dass in Ihrem Unternehmen die Betriebssystemkomponenten aller Computer laufend und systematisch aktualisiert werden?
7. Haben Sie auf allen Computern Virenschutzprogramme und werden diese laufend (täglich oder wöchentlich) aktualisiert?
8. Sind Sie sich der mit E-Mails zusammenhängenden erhöhten Risiken und der Notwendigkeit von Abwehrmaßnahmen bewusst (Virenschutzprogramm, Mitarbeiterschulung, Updates)?
9. Sind Sie sich beim Computer-Zugang ins Internet der Gefahren und der Notwendigkeit von Abwehrmaßnahmen bewusst (Firewall, Virenschutzprogramm, Mitarbeiterschulung, Updates)?
10. Haben Sie ein fachmännisch installiertes und laufend gewartetes Firewall-System im Einsatz, dessen Protokolle (Logfiles) regelmäßig überprüft und ausgewertet werden?

Firewall hat man sich bisher erfolgreich gegenüber Angriffen geschützt – was im Rahmen eines Tests durch die FH Sankt Pölten bestätigt wurde, schildert der Unit-Leiter Neue Medien & IT, Michael Schützenhofer.
Um auch bei der Datenübertragung den Kunden ein hohes Sicherheitsniveau zu bieten, hat gugler eine eigene Plattform für den Up- und Download entwickelt. Einerseits konnte man so die Mail-Clients entlasten und mit einer Verschlüsselung bei der Übertragung die notwendige Sicherheit gewährleisten, denn eine E-Mail sei nichts anderes als ein offener Brief, gibt Schützenhofer zu bedenken.
Von den zitierten Unternehmen abgesehen, ist bei Klein- und Mittelbetrieben jedoch grundsätzlich ein fehlendes Bewusstsein für das Thema IT-Sicherheit auszumachen. Viele sind der Meinung, dass es Hacker nur auf große Unternehmen abgesehen hätten. Das Netz sei aber längst von sogenannten Robots unterwandert, die automatisiert versuchten, alle über das Internet erreichbaren Computer auszuspähen. Daher ist ein regelmäßiges Monitoring der Firewall wichtig, um nachzuvollziehen, was sich am digitalen Eingang zur Firma tatsächlich abspielt.
Bei aller Technik dürfe man auch nicht die menschliche Komponente vergessen, wenn man das Thema IT-Sicherheit in den Griff bekommen will. Allerdings hält Michael Schützenhofer nichts davon, den Mitarbeitern etwa den Zugang zu Social-Media-Tools zu verwehren: »Wenn man heute als Unternehmen junge, dynamische Mitarbeiter gewinnen möchte und den zeitgemäßen Dialog mit den Kunden führen will, muss man ihnen auch die Möglichkeit bieten, Twitter, Facebook und Co zu nutzen. Allerdings sind für den Umgang klare Spielregeln aufzustellen, an die sich alle halten.«

Vertragen sich Cloud-Computing und IT-Sicherheit?

IT-Sicherheitsexperten sind der Meinung, dass Hacker immer den Weg des geringsten Widerstands suchen. Da nutze es nichts, wenn man über eine nach allen Seiten perfekt abgesicherte Firewall verfüge und daneben über Datenbanken und Portale die Anstrengungen auf dem Gebiet der IT-Sicherheit unterlaufe. Gerade hier sehen Experten Schwachstellen, wie man sie auch oft in der grafischen Industrie antrifft.
Vor allem Content-Management-Systeme, die auf Open-Source-Software setzen, haben sich als besonders anfällig erwiesen. Um IT-Sicherheit professionell in Angriff zu nehmen, bildet nach Profi-Tipps die ISO-Norm ISO 27001 eine hervorragende Grundlage, wobei auf eine Zertifizierung, die richtig ins Geld geht, im ersten Schritt durchaus verzichtet werden könne.
Auf die Frage, wie sich Cloud-Computing und IT-Sicherheit miteinander vertragen, meint Helmut Fidi, Senior Security Consultant bei der CoreTec IT Security Solutions GmbH, kurz und bündig: »Schlecht.« Als Anwender wisse man nicht, wo die Daten in der Cloud liegen, und man habe keine Garantie, dass die Daten nicht auch in falsche Hände gelangen könnten. Haftungsfragen im Zusammenhang mit Cloud-Computing seien auch noch nicht eindeutig geklärt.
Doch ist hier etwas mehr Differenzierung angesagt. Denn die Angebote für das Auslagern von Daten unterscheiden sich erheblich – wohl auch beim Thema Sicherheit.
So ist man bei HP, einem Unternehmen, das stark auf das Thema Cloud-Computing setzt, naturgemäß anderer Meinung. Dieter Kittenberger, Manager Enterprise Server, Storage & Networking, HP Österreich, meint:

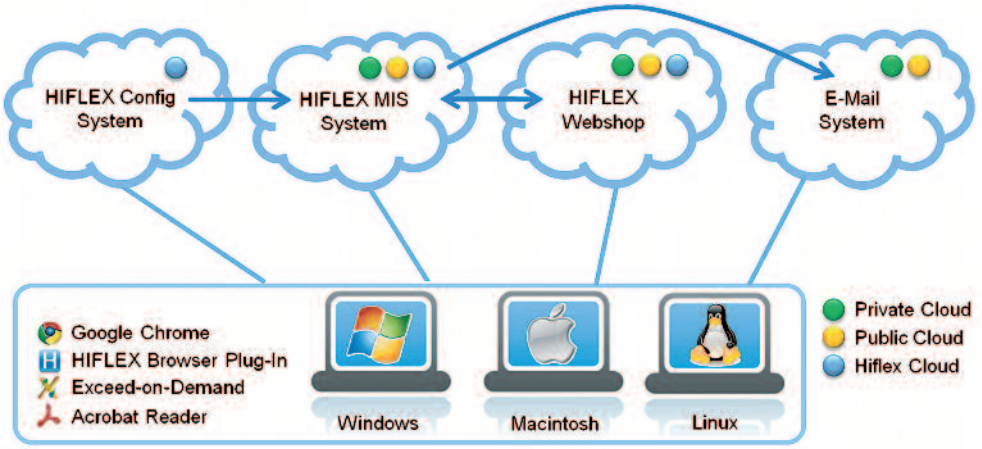


DATENZUGRIFF VON überall!

Los, alle auf die Bäume: Hiflex bietet seine mehrfach ausgezeichneten Softwarelösungen zur Automatisierung kaufmännischer und technischer Geschäftsprozesse jetzt im Internet an. Sie benötigen keine eigenen Server, Administratoren oder Speicherplatten mehr, sondern mieten bei Bedarf entsprechende Kapazitäten in der ›Wolke‹ an. Keine Investitionen in teure Infrastruktur, keine Lizenzen, sondern Miete: Software as a Service. Hiflex Enterprise Cloud Computing ermöglicht von überall und zu jeder Zeit den vollen Zugriff auf das Management Information System über das Internet. Flexibler. Günstiger. Sicherer.

www.hiflex.com

HIFLEX
MIS · JDF · Web-to-Print
Enterprise Cloud Computing



Bei der Hiflex-Lösung muss die Software nicht zwingend in einer ›Public-Cloud‹ oder ›Hiflex-Cloud‹ installiert werden, sondern kann in einer ›Private Cloud‹ betrieben werden. Sie bietet den Zugang zu abstrahierten IT-Infrastrukturen innerhalb der eigenen Organisation. Damit verbleiben die Daten nach wie vor im eigenen Haus auf eigenen Systemen (siehe auch unseren Beitrag in Heft 73, Seite 40).

»Die Rolle der Unternehmens-IT entwickelt sich immer mehr zu der eines ›Service-Brokers‹. Es gilt, die richtige Bezugsquelle für einzelne IT-Services zu finden.« Diese könnten entweder weiterhin in einer Private Cloud betrieben oder aus einer Public Cloud bezogen werden.
Experten sehen die Zukunft in sogenannten Hybrid-Modellen, bei denen Unternehmen Services und Applikationen je nach individuellen Anforderungen aus einer dieser Quellen beziehen. Dem Thema Sicherheit wird so optimal und sehr individuell Rechnung getragen, da so für jeden Service genau die Sicherheitsoptionen gewählt werden können, die den Bedürfnissen entsprechen.
So können beispielsweise für Daten mit hoher Sicherheitsrelevanz dedizierte Server und auditierbare Rechenzentren bestimmt werden, auch der Ort der Datenverwaltung kann vertraglich spezifiziert werden. Das Unternehmen definiert mit solchen Cloud-Lösungen die Kontrolle über bestimmte Teile seiner Daten. Standardisierte Services, beispielsweise Mail-Services, könnten hingegen aus einer Public Cloud bezogen werden. Mit einer solchen hybriden Lösung gewinnen Unternehmen Flexibilität und können Sicherheitslevels datenspezifisch festlegen.

Inhouse-Lösungen bevorzugt

Auch bei Hiflex, dem Entwickler des gleichnamigen MIS-Systems, sieht man erhebliche Vorteile des Cloud-Computings und bietet den Kunden individuelle und hybride Lösungen an. Dabei räumt Geschäftsführer Stephan Reichart ein, dass man keinen Kunden zu irgendeiner Lösung zwingen könne und wolle. Die meisten Kunden würden zunächst noch die Private Cloud bevorzugen, doch es sei nur eine Frage der Zeit, bis die Kunden selbst bei der Auslagerung sensibler oder unternehmenskritischer Daten einem Rechenzentrum vertrauen würden.

Advantage: Cloud

Die Kombination aus Virtualisierung, browserbasierter Nutzung im Internet und die Möglichkeit, solche Anwendungen auszulagern, sind die eigentlichen Vorzüge der ›Wolke‹.
So sehen viele Unternehmen den größten Vorteil von Cloud-Computing in der Tatsache, dass sie nicht in eigene Hard- und Softwareware samt Infrastruktur investieren müssen. Damit minimiert sich der Aufwand für Systemwartung und Personal – und das, obwohl die notwendige Performance und der Speicherplatz praktisch beliebig skalierbar sind. Hinzu kommt, dass die Sicherheit in einem professionellen Datenzentrum um ein Vielfaches höher ist, als es üblicherweise in der eigenen Umgebung realisierbar ist. Neben der Absicherung gegen Naturrisiken bieten Datenzentren Schutz gegen Einbruch, Vandalismus oder Sabotage, die Räumlichkeiten sind perfekt klimatisiert und verfügen über professionelle Brandschutzsysteme. Und selbst bei einem abrupten Stromausfall garantieren Notstromaggregate und Batteriespeicher die unterbrechungsfreie Versorgung.
Datenzentren bieten damit durchgehende Erreichbarkeit und die Verfügbarkeit der Dienste liegt dank 24/7-Überwachung und redundanter Systeme bei deutlich über 99%.
Externe Datenzentren bieten somit optimalen Schutz für die Daten, da Software, Rechenleistung und Speicherung über mehrere Server verteilt sein können.

Teil des Risikomanagements

Auch wenn die Sicherheit der Daten in einem Rechen- oder Datenzentrum gewährleistet ist, muss mit den Daten ja noch immer gearbeitet werden können. Niemand wird die Daten aus Angst vor Sicherheitslücken komplett wegschließen können. Deshalb müssen bei der täglichen Arbeit mit den Daten Rechte vergeben werden, damit nur die Mitarbeiter Datenzugriff haben, die entsprechend qualifiziert und autorisiert sind.
Die IT ist für Unternehmen heute also nicht mehr nur ein Motor zur Effizienzsteigerung, sondern auch ein Risikofaktor. Deshalb ist der Unternehmer gut beraten, der das Thema IT-Sicherheit dem Risiko-Management eines Unternehmens zuordnet.

KAMPF DEN SPAMS

Heutzutage ist im Schnitt weltweit nur noch jede zehnte E-Mail keine Spam-Mail! Organisierte Netzwerke versenden täglich Millionen unerwünschter Werbemails für Pharmaprodukte, ›fast echte‹ Luxusuhren oder Onlineglücksspiele.
Durch Spams entsteht alleine in den USA jährlich ein Schaden von rund 22 Milliarden $-Dollar. Viele Spammer packen Schadsoftware in ihre Mail ein, die sich nach Öffnung der Mail verselbstständigt und ähnlich wie ein Virus agiert. So werden viele PC-Benutzer unbewusst Teil eines Netzwerks, das von ihrem Rechner Spams und Schadsoftware weiter versendet.

Quark Publishing System 9

Design und Publishing für iPad, ePUB, Print, mobile Geräte und das Web

NEU: App Studio für Quark Publishing System

Ganz gleich, ob Sie Marketingmaterial, Finanzberichte, Publikationen für die technische Dokumentation, Zeitungen, Zeitschriften, Bücher oder andere Informationen über Printmedien, Websites oder mobile Geräte veröffentlichen, Quark Publishing System® kann Ihnen helfen, medienübergreifend Inhalte zeitnah und kostengünstig auszugeben.

App Studio ist ein optionales Modul für Quark Publishing System, das es Ihnen ermöglicht, mit Ihren vorhandenen Design- und Publishing-Werkzeugen iPad® Apps zu erstellen und zu veröffentlichen. Schnell, einfach und kostengünstig pro publizierter Ausgabe – ohne Jahresgebühren und ohne Download-Kosten.

App Studio für Quark Publishing System beinhaltet:

- Eine „Starter App" für das iPad, die der Ausgangspunkt für das Konfigurieren von kundenspezifischen iPad Apps ist
- Das iPad Framework, das es den Kunden ermöglicht, stark individualisierte und gebrandete Apps zu erstellen
- QuarkXPress XTension® Software zum Anreichern von Inhalten mit interaktiven Elementen, die im Dateisystem oder in Quark Publishing System gespeichert und verwaltet werden
- Einen web-basierten Service zum Verwalten von Apps, Publikationen und Ausgaben, jederzeit und an jedem Ort
- Funktionen zum Testen digitaler Publikationen im iPad Simulator von Apple® oder direkt auf einem iPad
- Automatisierungs-Workflows in Quark Publishing System zum Veröffentlichen und Aktualisieren digitaler Publikationen

Revolutionizing Publishing. **Again.**™

Quark