IT-SPIEGEL

Die Zeitung für den EDV-Bereich

netyard | KUNDENZEITUNG AUSGABE NR. 1/2014

IT-Sicherheit: Eine Schwachstellen-Analyse

Wie sicher ist die eigene IT-Landschaft? Welche IT-Bereiche bergen Gefahrenpotenziale und wo treten diese häufig auf?
Seite 2

Wolke im Sinkflug – Status quo des Cloud Computings

Verlangsamtes Wachstum: Die NSA-Affäre hat ein Jahr nach Bekanntwerden Spuren auf dem Cloud-Markt hinterlassen.
Seite 4

INTERN

Neue netyard-Mitarbeiter

netyard freut sich drei neue Mitarbeiter vorstellen zu dürfen. Als Unterstützung im Bereich Office ist Sandra Zipfel und in der Technik sind Daniel Gerdiken und Falko Ziemann zu dem netyard-Team hinzugestoßen.

Seit vergangenem November unterstützt Sandra Zipfel (36) das netyard-Office tatkräftig. Nach ihrem Abschluss zur staatlich geprüften Betriebswirtin (Fachrichtung Hotellerie) arbeitete sie 10 Jahre lang bei einer Unternehmensberatung als Leitung Office Management bis sie nach einer Elternzeit zu netyard wechselte.

Falko Ziemann (31) ist seit Februar 2014 als neuer Mitarbeiter im Technik & Support-Team tätig. Nach seiner Ausbildung zum Fachinformatiker Systemintegration arbeitete er u.a. als Systemadministrator bei einem ITK-Dienstleistungsunternehmen, als Consultant in einem Beratungsunternehmen für die Vernetzung von Prozessen, Informationen und Technologien sowie als selbständiger Consultant. Zuletzt war er als Projektleiter bei einem IT-Dienstleister in Wuppertal tätig, bis er die neue Stelle bei netyard besetzte.

Editorial

Liebe Kundinnen und Kunden,
die neue Leitstrategie „Mobile First – Cloud First“ des Softwareherstellers Microsoft geht an den Anforderungen vieler Unternehmen vorbei. Nach einer Studie von TecChannel, einem Online-Portal für IT-Entscheider, stimmen nur 49 Prozent der befragten Microsoft-Kunden der Aussage zu, dass die Fokussierung auf Cloud Computing-Services aus ihrer Sicht richtig und wichtig ist. Durch das Angebot der Cloud-Dienste will Microsoft aufgrund des Trends „Mobiles Arbeiten“ eine breitere Produktaufstellung erzielen. In Zeiten von NSA-Spähaffären stehen aber genau solche Dienste in der Kritik, eine offene Tür für Datenspione zu sein.

In unserem Leitartikel auf *Seite 2 „IT-Sicherheit: Eine Schwachstellen-Analyse“* hat sich netyard – auch in Folge der anhaltenden Meldungen über Sicherheitslücken diverser Großunternehmen – mit dem aktuellen Thema IT-Sicherheit beschäftigt und zusammengestellt, welche speziellen IT-Schwachstellen in kleinen und mittelständischen Unternehmen auftreten können.

Daniel Gerdiken (20) ist seit Anfang August letzten Jahres bei netyard neuer Auszubildender für den Beruf des Fachinformatikers Systemintegration. Zuvor erlangte er 2011 die Fachoberschulreife und besuchte im Anschluss ein Berufskolleg für den Bereich der Informatik. Wesentliche Schwerpunkte der Ausbildung bei netyard sind Backend-Systeme, Integration sowie Anwender-Support. ■

Zudem wurde über die bereits oben angesprochene Problematik ein Artikel *„Wolke im Sinkflug – Status quo des Cloud Computings“* auf *Seite 4* verfasst, der den momentan einsetzenden Imageverfall und Umsatzrückgang des Cloud-Geschäftes zum Gegenstand hat. ■

Kundenumfrage in eigener Sache

Der Servicegedanke und damit auch die Qualität der Dienstleistung spielt eine immer größere Rolle. Aus diesem Grund hat netyard, zusätzlich zu seiner monatlichen telefonischen Zufriedenheitsumfrage, eine weitere Kundenumfrage entwickelt, die die wichtigsten Merkmale in der Zusammenarbeit der Kunden mit netyard herausfiltern soll.

Dafür wurde ein Fragebogen erarbeitet, der neun Attribute (u.a. Reaktionszeit, Pünktlichkeit, Kommunikation, Verbindlichkeit uvm.) erfasst. Diese Attribute sollen in die vom Kunden persönlich richtige Gewichtung durch die Zahlen eins bis neun (1 = wichtig, 9 = unwichtig) gebracht werden. Die netyard-Techniker bringen bei Vor-Ort-Terminen den entsprechenden Fragebogen mit. Das Unternehmen hofft, dass Sie uns mit Ihrer Beteiligung eine ehrliche Rückmeldung Ihrer Einschätzung geben können und bittet Sie um Ihre Mitarbeit bei dieser Umfrage. ■

IT-Sicherheit: Eine Schwachstellen-Analyse

Der Stellenwert von Sicherheit für die eigenen Informations- und Kommunikationssysteme wird von kleinen und mittelständischen Unternehmen häufig unterschätzt. Sie sehen ihre Firma nicht als potenzielles Ziel von Internet-Kriminellen. Dabei sichert das Internet und die IT-Landschaft heutzutage allen Unternehmen – ob groß oder klein – die eigene Wettbewerbsfähigkeit auf dem Markt. Die Vernetzung durch das World Wide Web ist somit einerseits eine große Chance für Unternehmen, um mit Kunden und Geschäftspartnern in Kontakt zu treten und Geschäfte abzuschließen. Zum anderen birgt sie Risiken. Durch die digitalen Unternehmensprozesse entsteht eine Angriffsfläche für Attacken von Internet-Kriminellen. Kundendaten stehen digitalisiert zur Verfügung, die Kommunikation zwischen Kunden und Unternehmen findet häufig per E-Mail statt, im Online-Shop werden Produkte zum Kauf angeboten – jeder dieser Vorgänge kann mögliche IT-Schwachstellen beherbergen.

Sicherheitsvorkehrungen von Unternehmen sind häufig lückenhaft oder überhaupt nicht vorhanden. Dies hat die Wirtschaftsprüfungs- und Beratungsgesellschaft PricewaterhouseCoopers in einer Studie aus dem letzten Jahr herausgefunden. 405 Unternehmen und öffentliche Non Profit-Organisationen wurden im Rahmen der Studie befragt. Rund jedes fünfte der befragten Unternehmen ist mindestens einmal Ziel einer Cyberattacke geworden. Jedoch kann mehr als die Hälfte (58 Prozent) der Unternehmen nicht sagen, welcher Bereich bzw. welche Daten angegriffen wurden und wie die Auswirkungen dieser Attacke waren.

Verschärft wird diese Thematik zusätzlich durch die wachsende Bedeutung des mobilen Arbeitens. Die zunehmende Nutzung des Internets auf dem Smartphone oder Tablet PC im Büro und auch unterwegs intensiviert die Sicherheitsprobleme. Mit der seit Jahren wachsenden Zahl an Schwachstellen nimmt auch die Zahl derjenigen zu, die dies auszunutzen versuchen. „Die Liste der Angreifer aus dem Cyberspace wird länger“, sagt Steve Durbin, Geschäftsführer des Information Security Forums (ISF). „Sie reicht von Amateurhackern, über organisierte Kriminelle und Hacktivisten, die auf das Thema aufmerksam machen wollen, bis hin zu staatlichen Akteuren, die von Ländern mit großen Budgets finanziert werden.“

HÄUFIGE SCHWACHSTELLEN

- ✓ Mobile Endgeräte
- ✓ Online-Speicher, z.B. Dropbox
- ✓ Soziale Netzwerke
- ✓ Faktor Mensch
- ✓ Datensicherung
- ✓ Datensicherheit

Im Folgenden ist eine Liste mit den häufigsten Schwachstellen der IT-Sicherheit zusammengestellt, um die umfangreichen Gefahrengebiete für Unternehmen zu verdeutlichen: Der Grundstein für eine optimale IT-Sicherheit ist eine abgesicherte IT-Landschaft. Hierzu gehört vor allem ein aktueller Virenschutz für PCs und Laptops, die im Unternehmen genutzt werden. Regelmäßig durchgeführte Updates schließen neu gefundene Sicherheitslücken und sollten anhand von Vor- und Nachsorgeterminen überprüft werden. Zudem sollte ein IT-Sicherheitskonzept auf Geschäftsführerebene als strategischer Grundstein erarbeitet und umgesetzt werden. Dies inkludiert auch eine Strategie für ein Notfallmanagement in Krisensituationen, beispielsweise wenn der Server ausgefallen ist.

Wenn ein Glied in der Kette der IT-Sicherheit reißt, kann schnell das gesamte Sicherheitskonstrukt instabil werden.

Eine unvollständige bzw. nicht geplante **Datensicherung** muss als weitere Gefahrenquelle für die IT-Sicherheit in Betracht gezogen werden. Die sich in einem bestimmten Turnus wiederholende Datensicherung, auch Back-up genannt, sichert die Daten des gesamten IT-Systems auf einem anderen Speichermedium in Form einer Sicherungskopie. Da jedes Jahr das Datenaufkommen von Unternehmen weiter ansteigt, sollte auch dieser Faktor mit in die Back-up-Strategie integriert werden. Die Planung der Datensicherung sollte deswegen nicht nur mittelfristig, sondern auch langfristig und darüber hinaus flexibel, angelegt sein.
Datensicherung und **Datensicherheit** gehören immer zusammen und dürfen nie getrennt voneinander betrachtet werden. Denn den Zustand der Datensicherheit erreicht man über geeignete Maßnahmen der Datensicherung. Datensicherheit hat das technische Ziel, Daten jeglicher Art in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen zu sichern. Beide Bereiche haben damit eine zentrale Rolle in der IT-Sicherheit und können hierdurch leicht zur Schwachstelle werden.

Das **Arbeiten mit mobilen Endgeräten**, wie Notebooks und Netbooks, ist im Unternehmensalltag nicht mehr wegzudenken. Arbeitnehmer können dadurch Arbeitsplatz ungebunden im Büro, direkt beim Kunden oder von unterwegs aus arbeiten. Auf den Geräten befinden sich jedoch oftmals sensible oder sogar unternehmenskritische Daten. Aus diesem Grund ist das Gefahrenpotenzial einer Sicherheitslücke, wodurch Daten abgeschöpft werden können, in diesem Bereich der IT nicht zu unterschätzen.

Bequem unterwegs über Notebook oder Smartphone Geschäftsdokumente und Fotos abspeichern – Cloud-gestützte **Online-Datenspeicher,** wie z.B. Dropbox, erfreuen sich in Unternehmen immer größerer Beliebtheit. Aber die Nutzung dieser Online-Speicher kann zu vielen Sicherheitsproblemen in der Unternehmens-IT führen. Zum einen kann die IT-Abteilung die Datenhaltung nicht kontrollieren. Es entsteht Intransparenz und Dezentralisierung der Daten. Zudem mangelt es vielen Anbietern von Online-Speichern an ausreichenden Sicherheitsmaßnahmen, z.B. der integrierten Datenverschlüsselung. Zuletzt riet auch der Ex-Geheimdienstmitarbeiter Edward Snowden in einem Interview mit einer britischen Zeitung von dem beliebten Online-Speicher Dropbox ab. Als Grund nannte er den ungehinderten Zugriff der Dropbox-Mitarbeiter auf den Datenspeicher.
Im **Web 2.0** wird das Internet als interaktive Plattform genutzt, in Form von sozialen Netzwerken wie Facebook oder XING. Unternehmen sind dort mit Unternehmensprofilen vertreten und kommunizieren über diese mit ihren Kunden. Durch Sicherheitslücken in den sozialen Netzwerken oder einer Schadsoftware kann die Gefahr bestehen, dass Informationen und Daten ausspioniert werden.

Häufig ist ungewollt das menschliche Handeln eine Gefahrenquelle für die IT-Sicherheit: unbedachtes Herunterladen von Daten aus dem Internet, die Nutzung von mit Viren infizierten Laptops oder der unsorgfältige Umgang mit Passwörtern. Das grundlegende Verständnis sowie die Sensibilisierung für einen bewussten Umgang mit solchen Risikofaktoren ist aus diesem Grund der beste Lösungsweg. Unerfreulicher Weise ist die Erkenntnis für die **„Schwachstelle Mitarbeiter“** in kleinen und mittelständischen Unternehmen noch nicht vollständig angekommen. Die PwC-Studie hat ermittelt, dass 37 Prozent der befragten Unternehmen durch eine einmalige Unterweisung die Mitarbeiter über IT-Risiken aufklären – bei 11 Prozent gibt es sogar gar keine Schulung zu dem Thema. ■

netyard-Interview:
IT-Qualität und -Zuverlässigkeit haben oberste Priorität

Die Geschäftsbeziehung zwischen der Kanzlei ARNOLD RUESS Rechtsanwälte und netyard ist ganz frisch und existiert erst seit Oktober 2013. Das junge Unternehmen war auf der Suche nach einem neuen IT-Dienstleister in direkter Ortsnähe zum Büro und ist dadurch auf netyard aufmerksam geworden.

Im Interview erzählt der Partner der Sozietät Dr. Bernhard Arnold, wie netyard die Erneuerung der IT-Landschaft umsetzte und welchen besonderen Anspruch die Anwaltskanzlei an das IT-System hatte.

ARNOLD RUESS Rechtsanwälte

Die Kanzlei ARNOLD RUESS Rechtsanwälte wurde im März 2010 gegründet. Entstanden aus einer internationalen Kanzlei mit 3.000 Anwälten weltweit, haben sich die Gründungspartner Dr. Bernhard Arnold und Prof. Dr. Peter Ruess selbständig gemacht. Das Unternehmen ist auf dem Gebiet des gewerblichen Rechtsschutzes spezialisiert. Dies umfasst u.a. das Marken-, Patent- und Urheberrecht sowie Lizenz- und Vertragsgestaltung. Die Mitarbeiterzahl ist im Laufe der Zeit – von den anfangs zwei Mitarbeitern – auf neun Mitarbeiter angestiegen. Es sind momentan sieben Anwälte und zwei Assistenten in der Kanzlei beschäftigt.

ARNOLD RUESS
RECHTSANWÄLTE UND FACHANWÄLTE FÜR GEWERBLICHEN RECHTSSCHUTZ

Dr. Bernhard Arnold ist Gründungsmitglied und Partner der Sozietät. Sein fachlicher Schwerpunkt liegt insbesondere auf dem Patent- und Urheberrecht.

Welche Geschäftsprozesse sind bei Ihnen im Unternehmen EDV-gesteuert? Welche Bedeutung kommt der EDV bei ARNOLD RUESS zu?

Dr. Bernhard Arnold: Die EDV nimmt für uns eine zentrale Rolle ein. Aufträge werden von uns per E-Mail angenommen und die gesamte Korrespondenz vom Gericht an den Mandanten wird per E-Mail weitergeleitet und abgewickelt. Die Gerichtsschreiben werden von uns grundsätzlich eingescannt, damit sie dauerhaft auf dem PC verfügbar sind. Außerdem ist die Fristenverwaltung des Sekretariats EDV-gestützt. Im Allgemeinen kann man sagen, dass jede eingehende und ausgehende Post in unserem Unternehmen am Ende als Datei in unserem System gespeichert wird.

Welche Maßnahmen wurden von netyard ergriffen, um Ihr altes IT-System zu ersetzen?

Dr. Bernhard Arnold: Unsere IT-Landschaft war ein bisschen in die Jahre gekommen und lief nicht mehr rund. So dass wir durch diese häufig mehr behindert, als unterstützt wurden. Im Dezember 2013 wurde die alte IT-Umgebung dann durch eine neue von netyard abgelöst. Dafür wurde zusätzliche Hard- und Software eingekauft.

Partner von ARNOLD RUESS Rechtsanwälte: Dr. Bernhard Arnold

Für die neue IT-Landschaft wurde auch ein neues IT-Konzept realisiert, das mit einer vorherigen Beratung einhergegangen ist. In der Beratung haben wir dann genau die Bedürfnisse der Kanzlei analysiert und eine IT-Landschaft mit netyard zusammengestellt, die speziell auf unsere Anfor- derungen als Rechtsanwaltskanzlei eingeht.

Welche genauen Anforderungen haben Sie an Ihre geschäftliche IT-Landschaft?

Dr. Bernhard Arnold: Für uns ist sehr wichtig gewesen, dass, obwohl wir ein recht kleines Unternehmen im Gesamtmaßstab sind, bei IT-Qualität und -Zuverlässigkeit ein hohes Niveau angelegt wird. Die Wahrscheinlichkeit, dass irgendetwas ausfällt – seitens Hardware oder Internetleitung –, darf nie dazu führen, dass wir handlungsunfähig werden. Unsere „recht ordentlichen“ Stundensätze lassen es einfach nicht zu, dass ein Ausfall der IT die Arbeit behindert. Man kann sich leicht ausrechnen, was wir nicht verdienen, wenn durch eine Störung der IT, unsere sechs Anwälte nicht arbeiten können. Unsere Mandanten betrauen uns regelmäßig mit Fällen, die für sie sehr bedeutend oder sogar existentiell sind, so dass wir ihnen gegenüber auch in der Verantwortung stehen, jederzeit arbeitsfähig zu sein.

Aus diesem Grund investieren wir umfangreich in eine hohe Ausfallsicherheit der IT-Landschaft. Mit unserem ersten Ansprechpartner Herrn Kempa haben wir ein Szenario entwickelt, dass das System bei einem möglichen Ausfall schnell wieder zum Laufen bringt. Z.B. gibt es kein Hardware-Ersatzteil, auf das die Kanzlei tagelang warten müsste – um einen wichtigen Punkt des IT-Konzepts kurz aufzugreifen.

Wie reagiert netyard auf Ihren täglichen IT-Bedarf? Können Sie dies evtl. an einem konkreten Beispiel erläutern?

Dr. Bernhard Arnold: Zusätzlich zu unserem Austausch des alten IT-Systems durch ein neues, hat die Kanzlei auch die Räumlichkeiten gewechselt. Da wir ja zwei Internetleitungen haben – eben wegen der Ausfallsicherheit –, gab es deswegen für die Techniker von netyard jede Menge zu tun, bis beide Leitungen im neuen Büro auch stabil funktionierten. Für die Zwischenzeit hatte Herr Kempa eine dritte Internetleitung verfügbar gemacht, damit wir in der Übergangsphase auch keine Sekunde offline sein mussten. Dies ist ein gutes Beispiel für die Flexibilität, die netyard an den Tag legt, um unsere Kanzlei im Tagesgeschäft zu unterstützen. ■

BRANCHEN-NEWS

Microsoft-Support endet für Windows XP

Seitens Microsoft läuft die technische Unterstützung für das veraltete Betriebssystem aus. Am 8. April 2014 endete beim Betriebssystem Windows XP endgültig der Microsoft-Support. Seit diesem Tag stellt der Softwareriese keine Sicherheits-Updates mehr zur Verfügung und XP-Nutzer laufen stärker in die Gefahr ihren Rechner mit Viren oder Schadprogrammen zu infizieren.

Die technische Unterstützung für das mittlerweile zwölf Jahre alte Betriebssystem Windows XP hätte eigentlich schon 2011 eingestellt werden sollen. Da aber eine große Anzahl an Nutzern an diesem Betriebssystem festhielten, verlängerte Microsoft die Frist bis 2014. Einen „Nachschlag“ wird es jedoch auf keinen Fall geben, erklärte der Microsoft-Support gegenüber dem Online-Portal Neowin.

Für Cyberkriminelle ist Windows XP immer noch ein interessantes Ziel. Dies liegt unter anderem an der weiten Verbreitung des Betriebssystems. Das Marktfoschungsinstitut Net Applications hat herausgefunden, dass der Marktanteil von XP im Januar 2014 immer noch bei 29 Prozent lag. Nur Windows 7 hatte mit 47,5 Prozent einen höheren Anteil. ■

Wolke im Sinkflug – Status quo des Cloud Computings

Durch den Datenspionageskandal der NSA bekam im letzten Jahr das Hypethema „Cloud Computing" einen Dämpfer versetzt. Edward Snowden und seine Enthüllungen haben das Vertrauen in den Datenschutz erschüttert. Erst sah es kurzzeitig so aus, als ob Cloud Computing dies fast ohne Negativauswirkungen überstanden hätte. Als aber die Enthüllungen über Datenschnüffeleien nationaler Sicherheitsbehörden nicht abrissen, kratzte dies letztlich doch am Image der Wolke.

Eine Bitkom-Untersuchung aus Januar 2014 hat ergeben, dass 13 Prozent der Unternehmen konkret geplante Cloud-Projekte zurückstellen und 11 Prozent sogar bestehende Cloud-Lösungen aufgegeben haben. Dies bestätigt den leichten Abwärtstrend des IT-Nutzungskonzepts „Cloud Computing". Unternehmen schauen sich zunehmend nach sicheren Alternativen um. Der Public Cloud-Ansatz, bei dem externe Datenspeicherorte, z.B. im Ausland, verwendet werden, verliert damit an Attraktivität. Die logische Folge ist, dass Lösungen, wie u.a. in der Private Cloud, verstärkt in den Blickpunkt von IT-Entscheidern rücken. Denn hierbei werden Unternehmen für die eigenen Daten selbst zum Betreiber eines Cloud-Dienstes aufgrund des firmeninternen Datenspeichersystems.

Neue Alternativen sind gefragt

Die allgemeine Marktlage der Technologiewirtschaft hat Martin Weigert von netzwertig.com prägnant zusammengefasst: „Ich wünsche mir, dass wir momentan tatsächlich Zeuge einer Technologieblase werden, und dass diese mit einem Knall verschwindet. Ich wünsche mir ein Ende der meines Erachtens nach ungesunden Überhitzung der Webwirtschaft, welche den Fokus von Unternehmen und Investoren in großer Zahl auf Spielereien […] und auf die Verwandlung von Nutzern in gläserne, leicht manipulierbare Konsumenten lenkt."

Verlangsamtes Wachstum auf dem Markt: Graue Wolken ziehen über dem Himmel des Cloud Computings auf.

Paradigmenwechsel in Sachen Cloud

Aufbauend auf diesem Kommentar muss zusammenfassend gesagt werden, dass die Fälle von Datenspionage generell die Internetbranche und im Speziellen das Thema Cloud Computing verändert, sowie Unternehmen in Angelegenheiten des Datenschutzes in eine positive Richtung sensibilisiert, haben. Vordergründig sollte vor allem das Thema Sicherheit und der Schutz von Daten in ein verbessertes Cloud Computing-Modell eingearbeitet werden, um so ein Jahr nach den Datenspäh-Ereignissen einen Paradigmenwechsel einleiten zu können. ■

Krisen- und Prozessmanagement in der IT: Notfallplan im Worst Case

Brand im Serverraum, Stromausfall, Krankheitswelle von IT-Mitarbeitern, beschädigte Serverkomponenten – die Liste der Szenarien, die für Unternehmen zum Teil existenzbedrohend sein können, ist lang und kann durch viele weitere Risiken ergänzt werden. Ein durchdachter IT-Notfallplan, um die Informations- und Kommunikationstechnik dauerhaft zu gewährleisten, sollte aus diesem Grund in keinem Unternehmen fehlen. Aber der Notfallplan sollte nicht nur Maßnahmen in Krisensituationen enthalten, er sollte bereits zusätzlich präventiv Störereignissen entgegenwirken.

Daten sind in der heutigen Zeit zu einer Art neuen Währung für Unternehmen geworden. Sie entwickeln sich zu einem existenzbedrohenden Faktor, wenn z.B. durch einen Serverausfall auf Daten nicht mehr zugegriffen werden kann. Die Betriebsbereitschaft der IT bzw. deren Wiederherstellung nach einer Störung ist aufgrund dieser Tatsache wichtiger denn je geworden. Gewisse IT-Nutzungskonzepte, beispielsweise in der Public Cloud, erhöhen zudem die Wahrscheinlichkeit, dass solche Risiken eintreten und sollten daher im Rahmen einer Notfallplanung genaustens im Unternehmen diskutiert werden.

Ein Punkt in der Notfallplanung sollte sein, die Verantwortlichkeiten zwischen Geschäftsführung und IT-Abteilung in einem Ernstfall zu definieren. Es muss festgelegt werden, wer den Notfallplan initiiert, damit von Anfang an eine strukturierte Herangehensweise an das Problem besteht.

IT-Ausfall – Was ist im Notfall zu tun?

In der Konzeptionierung des IT-Notfallplans werden alle möglichen negativen Ereignisse festgehalten, um darauf aufbauend Handlungsoptionen beschreiben zu können. Damit greift ein Notfallplan auch immer in die Geschäftsprozesse ein und macht teilweise ein Prozessmanagement nötig.

In einer Risikobetrachtung werden zu Beginn des IT-Notfallkonzepts alle Störeinflüsse in einer Risikoanalyse festgestellt und bewertet. Die Dokumentation der Risiken in Bezug auf ihre Eintrittswahrscheinlichkeit und Wirkung stellt die Basis für jeden Plan dar.

Eine Checkliste beschreibt zudem für alle Mitarbeiter, wie im Ernstfall in vorgegebener Zeit durch vorgegebene Maßnahmen ein Notfallbetrieb und darüber hinaus die vollständige Betriebsbereitschaft hergestellt werden soll. Damit dies zügig und reibungslos umgesetzt werden kann, sollten alle Mitarbeiter in extra Schulungen im richtigen Umgang mit der Krise ausgebildet werden. ■

Impressum

netyard GmbH | Schanzenstraße 40 | 40549 Düsseldorf
Fon: 0211.415596-0 | Fax: 0211.415596-11
Mail: post@netyard.de | Internet: www.netyard.de
Geschäftsführer: Thorsten Dreiner, Florian Planert
Eingetragen beim Amtsgericht Düsseldorf, HRB 52 714
Fotoquellen: netyard GmbH, ARNOLD RUESS Rechtsanwälte, Himberry/photocase.de, Baweg/photocase.de

netyard
Ihr EDV-Systemhaus in Düsseldorf