Schadens-begrenzung

Marcel Knop

Die Liste möglicher IT-Sicherheitsvorfälle ist lang und reicht von gehackten Webseiten über nicht mehr erreichbare Dienste bis hin zu gestohlenen Datenbanken. Wie können betroffene Unternehmen darauf reagieren und worin unterscheidet sich der Umgang damit vom „normalen" Krisenmanagement?

iX-TRACT

- Cyberkrisen können beinahe jedes Unternehmen treffen und dessen Existenz bedrohen. Im Vorteil ist, wer sich frühzeitig auf den Ernstfall vorbereitet.
- Die erforderlichen reaktiven Fähigkeiten lassen sich mit geringem Aufwand in Organisationen implementieren. Das Lösen von Cyberkrisen ist nicht auf die IT-Abteilung beschränkt, da weitreichende Befugnisse sowie weitere Kompetenzen benötigt werden.
- Ein Schlüsselfaktor kommt in Krisensituationen der Unternehmenskommunikation zu: Sie entscheidet über Reputationsverlust oder auch -gewinn.
- Durch Cyberkrisenübungen lassen sich Mängel im Krisenmanagement effizient aufdecken und in tatsächlichen Fällen schneller überwinden.

Ob TV5 Monde, Sony Pictures, Vodafone, Target, Apples iCloud oder LinkedIn – beinahe täglich sind in den Medien Berichte über das Ausspähen von Kunden- und Kreditkartendaten, das Hacking interner Computersysteme und das erfolgreiche Angreifen von Infrastrukturen zu finden. Trotz aller Sorgfalt im präventiven Bereich lassen sich schwerwiegende IT-Sicherheitsvorfälle offensichtlich nicht vermeiden. Mangelhafte oder unübersichtliche Reaktionen können jedoch hohe materielle und immaterielle Schäden nach sich ziehen. Selbst Vorstandsmitglieder können dadurch mittlerweile ihren Posten verlieren, etwa Amy Pascal, frühere Co-Vorsitzende von Sony Pictures. Allerdings sind bis heute reaktive Fähigkeiten in vielen Unternehmen nicht oder nur schwach ausgeprägt vorhanden. Aufgrund der besonderen Komplexität von IT-Systemen und der meist besonders zeitkritischen Abläufe stellen Cyberkrisen besondere Anforderungen an die Bewältigungsstrukturen.

In der Behandlung von Sicherheitsvorfällen werden die Begriffe Störung, Notfall und Krise häufig verwendet, ohne dass immer ein einheitliches Verständnis zugrunde liegt. Daher folgt zunächst eine kurze Definition dieser Begriffe. Eine Störung ist die kleinste Form eines Vorfalls, der IT- oder Geschäftsprozesse beeinträchtigt. Beseitigt wird sie meist durch den IT-Support oder den jeweiligen Fachbereich selbst.

Von der Störung zur Cyberkrise

Bei einem Notfall handelt es sich um einen Vorfall mit wesentlicher Auswirkung auf den Betrieb des betroffenen Unternehmensbereichs. Zur Notfallbehebung müssen die Tätigkeiten des betroffenen Bereiches ganz oder teilweise unterbrochen werden. Es kommen vorbereitete Pläne aus dem Business Continuity Management (BCM) zum Einsatz, die dabei helfen, die ausgefallenen Ressourcen planmäßig wiederherzustellen und kritische Geschäftsprozesse im Notbetrieb fortzuführen. Diese Pläne basieren auf konkreten Ausfallszenarien.

Bedroht ein Vorfall die Existenz eines Unternehmens, spricht man von einer Krise. Besonderes Merkmal von Krisen ist ihre Unvorhersagbarkeit, sodass eine exakte Vorausplanung passender Gegenmaßnahmen – im Gegensatz zu Notfällen – nicht möglich ist. Die Krisenbewältigung erfordert weitreichende Handlungskompetenzen innerhalb des Unternehmens. Sie fin-

© Copyright by Heise Medien
Persönliches PDF für Marcel Knop aus 10119 Berlin

det daher immer mit Beteiligung der Unternehmensleitung statt. Da die rasch erforderlichen Entscheidungen teilweise auch die Unternehmensstrategie betreffen und somit nicht durch eine herkömmliche Aufbauorganisation getroffen werden können, werden Krisenstäbe einberufen.

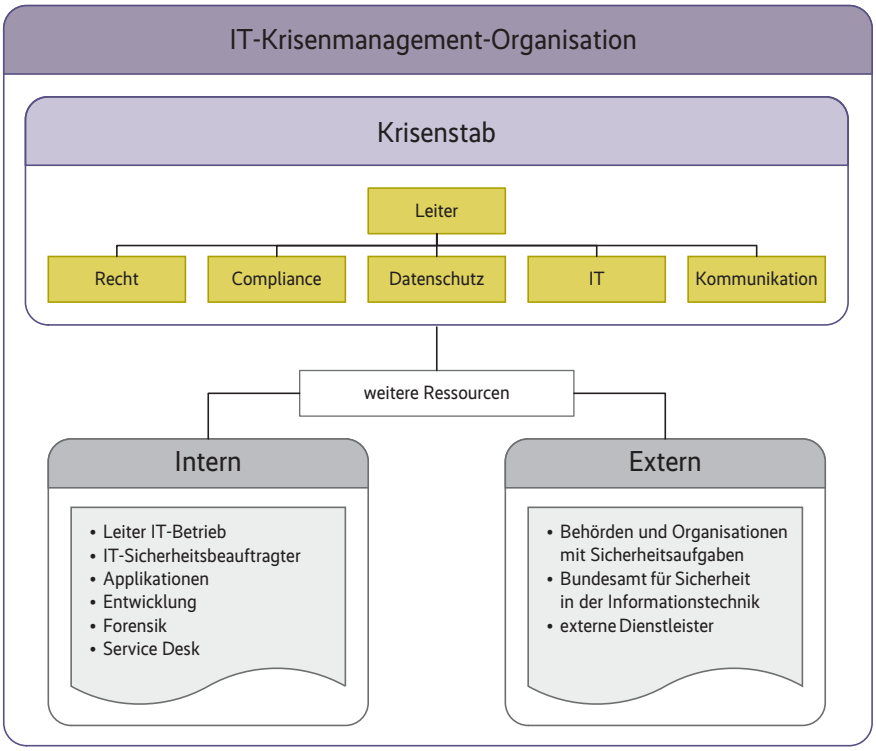
Cyberkrisen, also durch IT-Vorfälle ausgelöste Krisen, existieren erst seit relativ kurzer Zeit. Sie unterscheiden sich von herkömmlichen Krisen dadurch, dass sie besonders rasch Entscheidungen zur Eindämmung verlangen. Zudem erfordert ihre Bewältigung besonderes IT-Fachwissen, bedingt durch die Komplexität der zugrunde liegenden Systeme und Netze. Auch sind spezialisierte Juristen vonnöten, die in den wenigsten Unternehmen arbeiten.

Bildung eines Krisenstabs

Das typische Krisenmanagement in Unternehmen, organisatorisch angesiedelt im Bereich der Unternehmenssicherheit und personell meist besetzt mit Experten physischer Sicherheit und Kriminalistik, entscheidet bei Vorliegen einer potenziellen Cyberkrise häufig wegen der technologischen Komplexität, den Vorfall der IT-Abteilung zu übergeben. Diese wiederum verfügt in der Regel weder über Krisenmanagementkompetenz noch über die in dieser Situation notwendigen Befugnisse. Dadurch entsteht ein Zuordnungs- und Kompetenzgerangel, was die eigentliche Krisenbewältigung unnötig verzögert.

Ein Krisenstab als reaktive Sonderbewältigungsorganisation dagegen bündelt alle notwendigen Kompetenzen und ist durch seinen schlanken Aufbau mit wenigen Beteiligten rasch entscheidungsfähig (Abb. 1).

Seine Kernaufgabe ist es, Informationen über die Krise zu sammeln (Lageerhebung), auszuwerten und notwendige Entscheidungen schnell genug zu treffen. Letzteres sollte nach einem einheitlichen Schema erfolgen, beispielsweise nach dem FORDEC-Modell aus der Luftfahrt. Ein Krisenstab besteht aus einem entscheidungsbefugten Leiter sowie Vertretern der betroffenen Unternehmensbereiche. Weil er weitreichende Entscheidungskompetenzen für die Dauer der Krise benötigt, ist meist auch die Unternehmensführung vertreten.



Ein typischer Krisenstab besteht aus wenigen kompetenten Beteiligten, die weitere interne und externe Helfer heranziehen (Abb. 1).

Da Krisen selten auftreten und mit besonderem psychischem Stress verbunden sind, sollten alle vorgesehenen Mitglieder des Krisenstabs, insbesondere der Leiter, Schulungen über die Methodik des Vorgehens absolviert haben.

Neben der Informationsbeschaffung, -verteilung und -auswertung zum Beurteilen der Lage gehören zu den Aufgaben eines Krisenstabs das Entwickeln und Auswählen von Handlungsoptionen, die Wirksamkeitsüberprüfung der eingeleiteten Maßnahmen sowie die Kommunikation mit Kunden, Aufsichtsrat, Mitarbeitern, Behörden und der Öffentlichkeit.

Für das gesamte Informationsmanagement steht dem Krisenstab ein Lagezentrum zur Verfügung. Dessen Mitarbeiter sind allerdings nicht entscheidungsbefugt. Für die Arbeit des Krisenstabs sollte im Vorfeld schon nach geeigneten Räumlichkeiten gesucht werden. Nützliche Hilfsmittel zur Darstellung der Lage, beispielsweise Beamer oder Flipcharts, sollten verfügbar sein.

Die Arbeit des Krisenstabs besteht im zyklischen Wiederholen aller Tätigkeiten rund um die Lagebeurteilung und -bearbeitung. Um die Situation neu zu beurteilen, analysieren die Beteiligten im Rückblick abgeschlossene Vorfälle und

Anzeige

© Copyright by Heise Medien
Persönliches PDF für Marcel Knop aus 10119 Berlin

Maßnahmen der Krise nach folgenden beispielhaften Fragen: Welche (Sofort-) Maßnahmen wurden bereits eingeleitet? Und sollen diese fortgeführt werden oder sind Ergänzungen notwendig? Was ist der Stand der Maßnahmen und welche Auswirkungen haben sie? Gibt es neue Informationen zur Lage? Welche Auswirkungen hat die Krise bislang und welche sind noch zu erwarten? Wie viel Zeit bleibt, die Krise zu bewältigen? Sind Restriktionen oder Rahmenbedingungen für das weitere Vorgehen notwendig?

Die Lagebearbeitung beschäftigt sich mit der zukünftigen Entwicklung der Krise und Maßnahmen zur Bewältigung. Dazu zählt das Erstellen von Best- und Worst-Case-Szenarien, das Festlegen der grundsätzlichen Krisenmanagement- und der Deeskalationsstrategie sowie der Plan zur Rückkehr in den Normalbetrieb, das Delegieren definierter Maßnahmen an einzelne Krisenbehebungsteams und die Umsetzungs- und Wirksamkeitskontrollen (Lage-Updates).

Ihre Einschätzungen sollten die Beteiligten zu Beginn einer Krise sowie in regelmäßigen Abständen überprüfen – insbesondere wenn es neue Informationen gibt oder wesentliche Entscheidungen anstehen. Checklisten haben sich dabei als nützliches Mittel bewährt. Sie stellen sicher, dass alle relevanten Interessenvertreter und Themen berücksichtigt und keine wichtigen Punkte übersehen werden.

Aufgrund der Vielfältigkeit potenzieller Szenarien lässt sich eine fachlich detaillierte Vorgehensweise zur Bewältigung des Vorfalls, wie sonst häufig im Technikbereich zu finden, nicht vorab erstellen. Allerdings hat ein verallgemeinerter Ansatz den Vorteil, dass er universell anwendbar und somit für jeden Krisenfall nutzbar ist. Das Unternehmen erwirbt also die Fähigkeit, auf Ereignisse jeder Art flexibel zu reagieren.

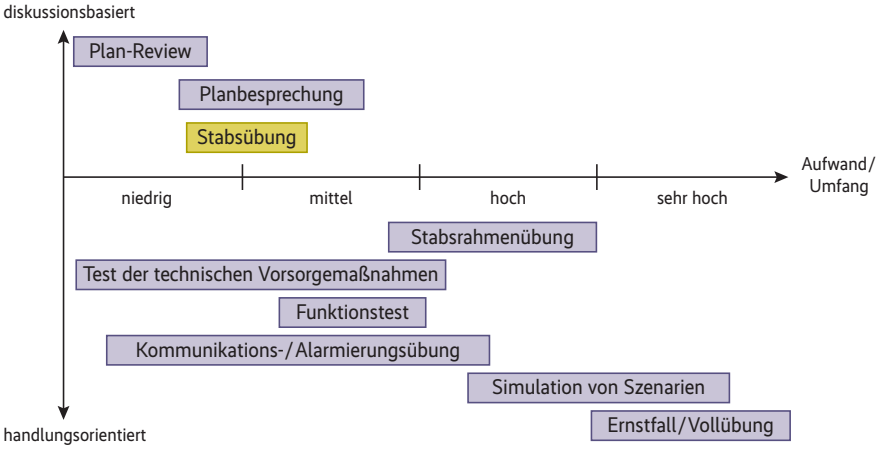
Da in einem Krisenfall mit dem Ausfall oder der Störung unternehmenseigener IT-Systeme zu rechnen ist, sollte ein Krisenmanagementplan, der alle Aktivitäten der Krisenbewältigung zusammenfasst, offline verfügbar sein. Alternativ kann man ihn bei externen Dienstleistern – angemessen abgesichert – aufbewahren.

Dokumentieren in mehrfacher Ausführung

In Krisensituationen müssen zum Teil weitreichende Entscheidungen innerhalb kürzester Zeit getroffen werden. Daher sollte sichergestellt sein, dass diese Entscheidungsprozesse nachvollziehbar dokumentiert werden. Zudem besteht insbesondere in Stresssituationen die Gefahr, dass die Beteiligten einzelne, aber wesentliche Punkte beim Krisenmanagement vergessen oder übersehen.

Auch hier haben sich Checklisten als probates Mittel erwiesen. Sie sollten mindestens die Themen Krisenstabsarbeit (personelle Besetzung und Arbeitszyklus des Stabs), Erstmaßnahmen (Dokumentation der Ausgangslage und initialer Maßnahmen) sowie IT-Forensik (zur Beweissicherung kompromittierter IT-Systeme) abdecken.

Vor allem in hektischen und stressigen Situationen des Krisenmanagements können die Beteiligten einschlägige Gesetze und Verträge sowie unternehmensinterne Regelungen leicht übersehen. Dabei sind alle Gesetze während einer Krise genauso zu beachten wie im Normalbetrieb, denn ein Verstoß führt zu den gleichen Rechtsfolgen. Lediglich einige Rahmenbedingungen, beispielsweise Stichtage für bestimmte Berichtspflichten, kann man in Absprache mit den zuständigen Behörden überschreiten.



Der Aufwand variiert je nach Teilbereich, der geübt werden soll (Abb. 2).

Um in der Krise stets gesetzeskonform zu handeln, empfiehlt sich daher, jedem Krisenstab einen Juristen beizustellen, der auf die rechtlichen Risiken der geplanten Maßnahmen im Entscheidungsfindungsprozess hinweist. Eine Übersicht der relevanten Gesetze ist im Rechtsregister des Unternehmens zu finden.

Verträge zwischen dem Unternehmen und seinen Kunden oder Zulieferern sollten Regelungen enthalten, wie in Krisenfällen mit den gegenseitigen Verpflichtungen umzugehen ist beziehungsweise auf welche Weise man eine Übergangsregelung finden kann. Allerdings zeigt die Praxis, dass derartige Regelungen nur selten in Vertragswerken zu finden sind.

Den größten gestalterischen Spielraum haben Unternehmen bezüglich interner Regelungen mit den Mitarbeitern. Allerdings gilt auch hier: Was vor der Krise mitbestimmungspflichtig durch den Betriebsrat war, ist es auch währenddessen. Dies betrifft insbesondere alle Maßnahmen, die eine direkte Auswirkung auf die Mitarbeiter selbst haben, beispielsweise zur Bekämpfung von Pandemiefällen, bei der von den Mitarbeitern Unterstützung und Kooperation gefordert ist. Der Betriebsrat sollte daher bei der Entwicklung von Krisenmanagementplänen und auch im Ernstfall im Krisenstab vertreten sein.

Kommunikation gezielt steuern

Von besonderer Bedeutung in einer Krise ist die Kommunikation. Sie kann die nicht materielle Auswirkung und öffentliche Wahrnehmung maßgeblich beeinflussen. Ziel ist, dass betroffene Unternehmen den Interpretationsrahmen der Krise selbst gestalten, bevor Medien oder andere Dritte es tun. Im schlimmsten Fall kann das Unternehmen die Deutungshoheit in der öffentlichen Diskussion verlieren und unglaubwürdig oder inkompetent erscheinen. Gerade durch die sozialen Medien wie Facebook und Twitter ist diese Gefahr latent vorhanden.

Einige Grundregeln haben sich bei der Unternehmenskommunikation bewährt. Hierzu zählt die „One-Voice-Strategie“, die die Kommunikationskanäle und Freigabeverfahren vereinheitlicht und festlegt. Ein entschlossenes und eindeutiges Handeln schafft Vertrauen in die Fähigkeit des Unternehmens, mit der Krise umzugehen. Zudem sollten ausschließlich gesicherte Fakten nach außen mitgeteilt werden, da Unwahrheiten meist recht schnell auffliegen.

© Copyright by Heise Medien
Persönliches PDF für Marcel Knop aus 10119 Berlin

In Krisenfällen ist mit besonders aggressiven Fragen aller Interessenparteien und der Öffentlichkeit zu rechnen. Trotzdem sollte der Kommunikationsverantwortliche aktiv und positiv formulieren und ehrliches Mitgefühl gegenüber den betroffenen Parteien zeigen.

Pressestatements sind eine gute Basis, Betroffene über die Lage zu informieren. Dabei sollte man einige Kernelemente nennen. Hierzu zählen die Beschreibung des aktuellen Ereignisses, das Äußern von Betroffenheit, falls es Geschädigte gibt, und gegebenenfalls Hinweise darauf, wie man nach den aktuellen Erfahrungen das Sicherheitskonzept im betroffenen Bereich weiterentwickeln wird. Fragen nach der Ursache oder Schuld sollte man zunächst nicht beantworten.

Reagieren statt blockieren

Sind die genauen Hintergründe des Vorfalls in der ersten Phase der Krisenbewältigung noch unklar oder dürfen aufgrund laufender Ermittlungen noch keine Details genannt werden, kann man gezielt vorläufige Stellungnahmen (Holding Statements) einsetzen. Diese sollen nur als Reaktion auf externe und interne Anfragen dienen. So lässt sich unter anderem die Antwort „kein Kommentar“ vermeiden, die in der Regel negativ und unter Umständen sogar als Schuldeingeständnis interpretiert wird.

Vorläufige Stellungnahmen umreißen inhaltlich kurz und knapp das Ereignis und beschreiben – sofern erfolgt – erste Maßnahmen in allgemeiner Form. Sie verraten nichts über Ursachen, zukünftige Maßnahmen sowie mögliche Entwicklungen und Auswirkungen des Vorfalls.

Zu Beginn einer Cyberkrise entsteht ein Informationsvakuum, das rasch zu füllen ist, damit das Unternehmen den Interpretationsrahmen der Ereignisse vorgeben oder aktiv mitgestalten kann.

Die folgenden Fragen werden mit hoher Wahrscheinlichkeit im Zusammenhang mit jedem Krisenszenario gestellt: Was ist passiert und wann? Wo fand der Vorfall statt? Warum und wie konnte es dazu kommen? Wer ist betroffen? Welche Konsequenzen zieht das Unternehmen daraus? Der Krisenstab sollte schnellstmöglich Antworten auf diese Fragen finden und sie adressatenspezifisch (Mitarbeiter, Kunden, Behörden, Presse et cetera) aufbereiten lassen.

Eine wesentliche Rolle beim Verbreiten des Interpretationsrahmens von Cyberkrisen spielen die sozialen Medien. Und ihre Relevanz nimmt weiter zu, sobald Cyberkrisen öffentlich werden und Gegenstand der Online-Debatte sind.

Bei dieser sollte die Kommunikation mit den Benutzern stets auf Augenhöhe erfolgen. Mögliche Konflikte sollten nicht offensiv ausgetragen und kritische Inhalte oder Negativmeldungen nicht zensiert werden. Auch sollte das betroffene Unternehmen laufende Online-Kampagnen auf ihre Angemessenheit hinsichtlich der Krisensituation überprüfen.

Cyberkrisen können durch soziale Medien zu einem großen öffentlichen Interesse führen. Aufgrund des hohen Kommunikationsaufkommens kann es zweckmäßig sein, mehrere Kommunikatoren einzusetzen und von der One-Voice-Strategie, die eine Freigabe jeder einzelnen Meldung vorsieht, zu einer One-Mind-Strategie zu wechseln. Bei dieser dienen Rahmenanweisungen (etwa Sprachregelungen, FAQs und Verfahrensanweisungen) für die „Unternehmenssprachrohre“ dazu, eine einheitliche Krisenkommunikation sicherzustellen.

Um die Wirksamkeit von Maßnahmen zum Cyberkrisenmanagement zu überprüfen, Schwachstellen aufzudecken und die Reaktionsgeschwindigkeit im Ernstfall zu erhöhen, haben sich Übungen als effektives Mittel erwiesen. Diese eignen sich zudem als Sensibilisierungsmaßnahme für Mitarbeiter in Sachen Krisenmanagement. Das Spektrum der Übungsmöglichkeiten, mit denen man Krisenmanagementpläne und -organisation testen kann, ist groß und reicht von einzelnen Funktionstests bis hin zu Vollübungen (Abb. 2).

Übungen sind in der Regel komplexe Vorhaben und bedürfen daher für einen reibungslosen Verlauf einer sorgfältigen Vorbereitung. Zudem sollte jede Übung dokumentiert werden, damit eine Nachbereitung möglich ist. Da die Übung nur dann zum gewünschten Ziel führt, wenn Verbesserungen in Krisenmanagementorganisation und Planung einfließen können, ist dieser Schritt besonders wichtig.

Orientierungshilfe: Standards und Normen

Für das Krisenmanagement existiert derzeit der deutsche Standard 100-4 des Bundesamts für Sicherheit in der Informationstechnik. Er behandelt jedoch die Themen Notfall- und Krisenmanagement gemeinschaftlich. Von der zukünftigen Überarbeitung ist eine Trennung der beiden Themen zu erwarten, die ihre jeweiligen Eigenheiten besser berücksichtigt.

Während für das betriebliche Kontinuitätsmanagement (Business Continuity Management, BCM) eine Reihe von Standards und Implementierungsspezifikationen existieren, gibt es für das Krisenmanagement bislang nur den „British Standard BS 11200, Crisis management. Guidance and good practice“. Er richtet sich an die Unternehmensleitung und behandelt das Etablieren eines strategischen Krisenmanagements.

Noch steckt der deutsche Versicherungsmarkt zur Absicherung von Cyberrisiken in den Kinderschuhen. Klassische Versicherungen bieten für diese relativ neuen Risiken derzeit meist noch keinen ausreichenden Schutz. Durch Hackerangriffe, IT-Ausfall und Datenverlust drohende Schäden waren stets ausgeschlossen. Dabei können durch einen Cybervorfall erhebliche direkte und indirekte Kosten entstehen.

Dazu zählen die Aufwendungen für die Wiederherstellung von Daten und Systemen nach einem Hackerangriff, die Honorare für IT-Forensiker zur gerichtsfesten Aufbereitung des Vorfalls sowie für spezialisierte Juristen, Krisen- sowie PR-Manager, die für Aufarbeitung und Bewältigung der Krise benötigt werden. Wenn Kreditkartendaten von dem Vorfall betroffen sind, ist zudem mit Vertragsstrafen aus den Haftungsvereinbarungen der Kreditkartenindustrie zu rechnen.

Neue Versicherungen schließen Lücken

Spezielle Cyber-Risk-Versicherungen können die Lücke schließen, die die bisherigen Versicherungssparten nicht abdecken. In Deutschland gibt es bereits ein Dutzend Versicherungsgesellschaften, die Schäden durch Cyberangriffe versichern. Der physische Verlust durch einfaches Liegenlassen oder Stehlen einer Festplatte mit Firmendaten ist dabei ebenso berücksichtigt wie das gehackte Firmenkonto, die Erpressung mit gestohlenen Daten oder die Betriebsunterbrechung durch IT-Ausfälle.

Zusätzlich bieten viele Versicherungen Präventionsmaßnahmen und Krisenübungen an, damit ihre Kunden im Fall der Fälle vorbereitet sind. Wesentlicher Bestandteil dieser Policen ist die Unterstützung durch erfahrene Krisenmanager, die im Ernstfall sofort zur Verfügung stehen und einen professionellen Umgang mit der Krise sicherstellen. (ur)

Marcel Knop

ist Managing Consultant bei HiSolutions in Berlin.

© Copyright by Heise Medien
Persönliches PDF für Marcel Knop aus 10119 Berlin