Risikomanagement in der IT unter Berücksichtigung der **Netzwerküberwachung**

White Paper
Autor: Dirk Paessler

Veröffentlicht: August 2008

www.de.paessler.com
info@paessler.com

PAESSLER®
the network monitoring company

CONTENTS

EINFÜHRUNG

Das Leben ist voller Risiken. Nachdem es unmöglich ist, diese völlig auszuschalten, werden vorausschauende Unternehmen Ressourcen einplanen, um Risiken zu minimieren und mögliche Verluste zu kontrollieren.

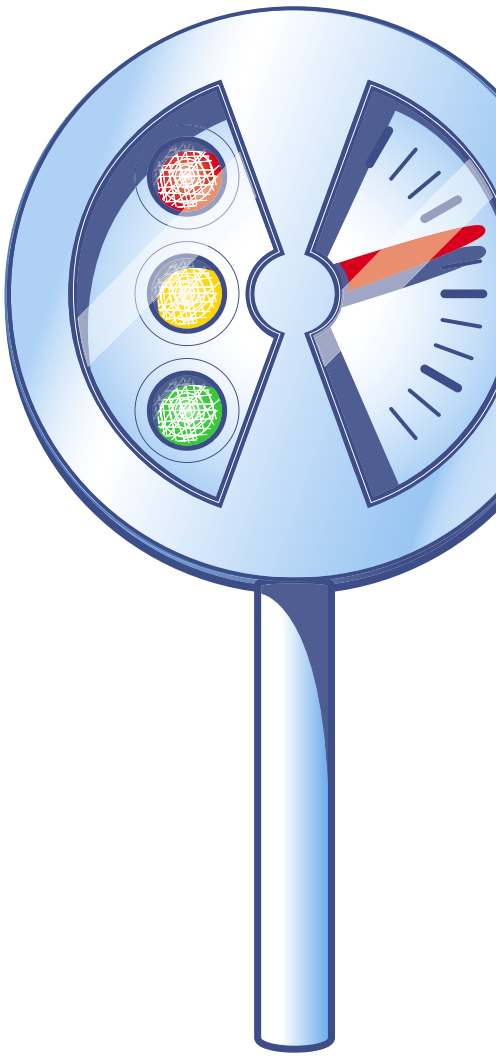
Im traditionellen Geschäftsleben heißt das Synonym für Risikomanagement in der Regel Versicherung. In der IT liegt der Fokus auf der technischen Behebung eines auftretenden Problems, zumeist ohne große Vorausplanung. Dass diese Vorgehensweise gravierende Nachteile mit sich bringt, liegt auf der Hand. So werden beispielsweise bei auftretenden Problemen wichtige Ressourcen bei der Problembehebung gebunden.

Darüber hinaus tendiert die IT dazu, sich auf zwei Arten von Risiken zu fokussieren: Malware (Viren, Trojaner & Co.) und Datenverluste (verursacht durch Malware oder Hardwaredefekte). Dies führt häufig dazu, dass andere Risiken völlig ignoriert werden, die aber letztlich nicht weniger Aufmerksamkeit erfordern
(dazu: “IT Risk Management: A Little Bit More Is a Whole Lot Better” unter www.gartner.com).

Auf der anderen Seite kann ein Zuviel an Risikomanagement Ressourcen binden, die sinnvoller in anderen Bereichen eingesetzt werden könnten. Entscheidend ist, die richtige Balance zu finden und Ressourcen überlegt einzusetzen um eine maximale Risikominimierung bei minimalen Kosten zu erreichen.

Die Bedeutung der Netzwerküberwachung für viele Bereiche des Risikomanagements in der IT wird oft unterschätzt und vernachlässigt. Natürlich wird in Netzwerküberwachungs-Software investiert, um defekte Switche und überlastete Leitungen zu identifizieren. Hier liegt jedoch weit mehr Potential vor, wie beispielweise das Entdecken unzulässiger Downloads, das Optimieren des kompletten Netzwerks und somit eine Beschleunigung der gesamten Geschäftsprozesse oder auch ein zusätzlicher Sicherheitsfaktor durch das frühzeitige Erkennen ungewöhnlicher Aktivität (Malware!). In einer Welt, in der Verzögerungen von Sekundenbruchteilen bei der Datenübertragung oftmals entscheidende Auswirkungen haben, können diese Faktoren den Ausschlag geben.

Eine umfassende und sehr detaillierte Untersuchung zu IT-spezifischen Risiken findet sich in der CobiT-Studie (Control Objectives for Information and related Technology) 4.1 der ISACA (Information Systems Audit and Control Association) unter dem Link www.isaca.org/CobiT. Diese Untersuchung beschäftigt sich mit IT-spezifischen Risiken unter besonderer Berücksichtigung des Netzwerkbetriebs. Sie verfolgt einen dreistufigen Ansatz zur Identifizierung, Beurteilung und Planung einer umfassenden IT-bezogenen Risikominimierungs-Strategie. Dabei weist sie der Netzwerküberwachung eine Schlüsselrolle zu.



Links

Gartner Group:
“IT Risk Management: A Little Bit More Is a Whole Lot Better”
www.gartner.com

ISACA:
CobiT-article on risk management
www.isaca.org/CobiT

ZUR KLASSIFZIERUNG IT-SPEZIFISCHER RISIKEN

Zunächst die schlechte Nachricht: Risiken lassen sich nicht ausschalten. Das Ziel des Risikomanagements ist Probleme zu identifizieren, die minimiert werden können (und sollten) und die Kosten zu deren Minimierung auf einem Level zu halten, das für das Unternehmen akzeptabel ist. Dies beinhaltet aber immer ein unvermeidliches unternehmerisches Restrisiko.

Kleine und mittlere Unternehmen (KMUs) können dabei mit unwahrscheinlichen, aber existenzbedrohenden Risiken konfrontiert werden, die akzeptiert werden müssen, da der Aufwand zur Vermeidung dieser Risiken für das Unternehmen nicht tragbar wäre.

Bedauerlicherweise agieren gerade KMUs im IT-Bereich bei ihrer Sicherheit häufig nur „Gefahren-bezogen“ ohne wirklich vorausplanendes Risikomanagement: Computerviren werden zur Gefahr, die IT installiert Anti-Virus Software; Trojaner werden zur Gefahr, die IT installiert eine Firewall und so weiter.

Diese Vorgehensweise bringt vor allem zwei Probleme mit sich:

- Erstens ist sie kurzsichtig: Sie beachtet nur einen Teil des Gesamtrisikos – normalerweise die technisch lösbaren Risiken.

- Zweitens unsystematisch und reaktiv: Sie führt zu einer Anhäufung von Hard- und Software, jede davon nur für ein Problem angeschafft, ohne zentrales Management oder durchgängiges Konzept. Eine IT-Abteilung, die ständig nur „Feuerwehr spielt“, kann niemals wirklich erfolgreich sein. Hier muss ein Schritt zurück gemacht und ein Risikoplan entwickelt werden.

RISIKO-KATEGORIEN

Die IT ist im Wesentlichen mit drei Kategorien von Risiken konfrontiert:

Technische Risiken

Technische Risiken sind die traditionellen Belange der IT, die von Viren-verursachten Ausfällen bis hin zu „exotischeren“ Fällen wie Denial-of-Service-Attacken oder sogenannten „War Walkers“ reichen. Mit War Walkers werden Hacker bezeichnet, die von außerhalb des Firmengebäudes in Funknetzwerke eindringen.

Die meisten Maßnahmen gegen diese Probleme sind ebenfalls technischer Natur, allerdings sind strenge Unternehmensrichtlinien in diesem Bereich ebenfalls von entscheidender Bedeutung. Dass Firewalls und Anti-Viren-Systeme auch auf mobilen Geräten installiert werden, ist dabei noch eine relativ offensichtliche Maßnahme. Dass Mitarbeiter keine unkontrollierten (und oft ungeschützten) WiFi-Knoten installieren können, wäre hier eine weitere sinnvolle Richtlinie.

Eine leistungsfähige Lösung zur Netzwerküberwachung wie beispielsweise PRTG Network Monitor der Paessler AG kann ungewöhnliche und somit verdächtige Aktivität im Netz frühzeitig erkennen und über die reine Warnung hinaus auch gleich den Verursacher identifizieren.

Rechtliche und personelle Risiken

Hier ist die Rede von der Vorbereitung auf eventuelle rechtliche Forderungen, unter die beispielsweise die Archivierung des E-Mail-Verkehrs fällt. Aber auch Mitarbeiter, die illegale Downloads über ihren betrieblichen Internetzugang tätigen oder potenzielle Spionage oder Sabotage durch Angestellte spielen hier eine Rolle.

Diese Gefahren sind schwerer zu handhaben, da die Technik hier keine eindeutigen Lösungen liefern kann. Strenge Unternehmensrichtlinien und eine gute Personalführung sind die Schlüssel zur Minimierung dieser Risiken.

Vorgesetzte sollten ausreichend in Personalführung geschult sein. Die Vorstellung, dass ein guter Angestellter nur mittels Beförderung ein guter Vorgesetzter wird, ist ein landläufiger Irrtum.

Auch hier kann professionelle Netzwerküberwachung bei richtigem Einsatz einige potenzielle Risiken minimieren. So bietet beispielsweise PRTG Network Monitor über eine Vielzahl von WMI-Sensoren die Überwachung von Exchange-Servern, liefert kontinuierlich Livedaten zu Art und Umfang des Netzwerkverkehrs und warnt aktiv bei Auffälligkeiten und Veränderungen.

Natürliche und von Menschen verursachte Katastrophen

Überschwemmungen, Brände oder Sturmschäden sind zwar nicht sehr wahrscheinlich, haben aber, wenn sie dann doch auftreten, umso dramatischere Auswirkungen.

Adäquate Strategien für diese Risiken zu finden gehört zu einer der schwierigsten Aufgaben des Risikomanagements.

Angeboten werden zahlreiche Strategien zu unterschiedlichsten Preisen und mit verschiedenen Schutzstufen. All diese Strategien müssen in Zusammenhang mit der Gesamtsituation des Unternehmens beurteilt werden.

Vor allem sollte Katastrophenmanagement mit gesundem Menschenverstand angegangen werden.

In der vernetzten Welt von heute können selbst relativ kleine Unternehmen ihre Datenzentren in modernen, sicheren Einrichtungen weit entfernt von katastrophengefährdeten Gebieten einrichten (unter Umständen gemeinsam mit anderen Unternehmen). Ebenso können existenzielle IT-Funktionalitäten in Form von SaaS (Software-as-a-Service) an Dienstleister ausgelagert werden, die ein deutlich höheres Sicherheitsniveau gewährleisten können, als das Unternehmen dies im eigenen Haus zu vertretbaren Kosten schaffen kann.

Auch bei der Minimierung dieser Risiken spielt eine zuverlässige Netzwerküberwachung, wie sie PRTG zu leisten imstande ist, eine nicht zu unterschätzende Rolle. Egal, ob das Unternehmen sein Rechenzentrum in Eigenregie auslagert oder als Service an einen Dienstleister vergibt: Eine ständige Verfügbarkeit und maximale Leistung beim Datentransfer sind essenzielle Anforderungen an ein externes Rechenzentrum und nur ein kontinuierliches und verlässliches Monitoring kann dies gewährleisten.

EIN DREI-STUFEN-PLAN

Auch wenn zahlreiche kleinere IT-Unternehmen und -Abteilungen die Planung ihrer Risikominimierung völlig vernachlässigen, ein Zuviel an Planung ist ebenso wenig sinnvoll. Vor allem KMUs, aber oft auch größere Unternehmen können ihr Risikomanagement durchaus schlank und formlos planen.

Stufe 1: Risikoauflistung und Kostenabschätzung

Der erste Schritt eines strategischen Risikomanagements ist, die Hauptrisiken der drei oben genannten Risikokategorien zu identifizieren.

Es gibt verschiedene Standard-Risikolisten; eine der komplettesten ist in der CobiT-Studie enthalten. Allerdings sind diese meist viel zu umfangreich und umfassend für die Belange einer IT-Abteilung oder eines kleineren IT-Unternehmens.

Jedes Projekt beinhaltet eine Reihe eigener, spezifischer Risiken, die Gefahr eingeschlossen, dass die Aufgabe niemals oder mangelhaft abgeschlossen wird oder dass Budget und Zeitplan überzogen werden.

Die reine Erstellung einer Liste aller Risiken ist in der Regel relativ einfach, eine Beurteilung dieser Risiken in Hinblick auf potenzielle Kosten und Bedeutung für das Unternehmen ist dagegen schon deutlich schwieriger. Während Risikolisten im Allgemeinen universell einsetzbar sind, können die Kosten, die durch diese Risken verursacht werden, von Unternehmen zu Unternehmen deutlich variieren.

Für Finanzunternehmen beispielweise können kleinste Verzögerungen bei der Transaktionsübermittlung gravierende Auswirkungen haben, während Unternehmen der produzierenden Industrie hier meist eine höhere Toleranz haben, dafür aber in hohem Maß von der Performanz ihrer ERP-Systeme abhängen. Dies erschwert eine genaue Abschätzung der Kosten einzelner Risiken für das jeweilige Unternehmen.

Der für die Risikoplanung Verantwortliche wird versuchen, möglichst viele Informationen sowohl von Entscheidern seines Unternehmens als auch von Branchenorganisationen oder von Kollegen anderer Unternehmen seiner Branche einzuholen.

Die Kostenabschätzung muss nicht präzise sein, wichtig ist zunächst, überhaupt eine Schätzung zu haben. Diese ist die Basis für die Entscheidung, welcher Aufwand

in die Risikominimierung investiert werden soll. Außerdem muss festgelegt werden, was für den Schutz des Unternehmens vor Standardgefahren wie Viren und Trojaner eingeplant werden muss.

Die wichtigen Fragen für den Planenden sind:

Wie viel soll für die Standards im Vergleich zu anderen Risiken eingeplant werden?

Wann übersteigen die Ausgaben den Kosten-Nutzen Rahmen?

Die Antworten auf diese grundlegenden Fragen hängen nicht zuletzt von den Kosten ab, die im Schadensfall durch die IT-Risiken verursacht werden können.

Ebenfalls mit einbezogen werden muss die Wahrscheinlichkeit, dass der entsprechende Schaden eintritt. So sind beispielsweise Viren ein ständiges Problem, wobei der einzelne Virus in der Regel keine großen Schäden verursacht und mit relativ geringem Aufwand beseitigt werden kann. Katastrophen sind weit weniger wahrscheinlich, können aber, so sie denn auftreten, ein Unternehmen vollständig ruinieren.

Stufe 2: Kostenminimierung

Eine erste Kostenabschätzung muss keine exakten Zahlen beinhalten – es ist nicht nötig, hier bereits Kostenvoranschläge einzuholen. Grobe Schätzungen anhand einer Internet-Recherche oder anhand von Erfahrungswerten sind völlig ausreichend. Wichtig ist, neben den aufzuwendenden Geldern auch die Kosten für die benötigte Arbeitszeit der involvierten Mitarbeiter zu berücksichtigen. Solange sich die Risikominimierung auf Kauf und Installation von Hard- und Software beschränken lässt, ist eine Kostenabschätzung sehr einfach. Darüber hinaus und insbesondere für den Katastrophenfall existieren verschiedenste Strategien zu unterschiedlichen Kosten und von unterschiedlicher Effizienz.

Bei der Entscheidung, welche Strategie für das eigene Unternehmen die geeignetste ist, müssen verschiedene Faktoren berücksichtigt werden:

- Tolerierbarkeit langer Ausfallzeiten
- verfügbare Ressourcen zur Problemlösung
- das Potenzial des Unternehmens, eine größere Katastrophe zu überstehen (Risikotoleranz)

Ein kleines Unternehmen, das nicht in der Lage ist, eine Katastrophe zu überstehen, würde mit dem Aufbau eines externen Rechenzentrums zur Datensicherung und -wiederherstellung (DR – data recovery) Geld verschwenden. Kann sich das Unternehmen nicht mehr als eine regelmäßige Datensicherung auf Datenträger leisten, so wird diese Sicherung eben zur DR-Lösung des Unternehmens, ob sie nun die tatsächlichen DR-Anforderungen des Unternehmens erfüllt oder nicht. Hier können Alternativen wie SaaS-Anbieter eine interessante Option sein.

Bei der Planung zur Risikominimierung kann sich auch herausstellen, dass die Kosten zur Minimierung mancher Risiken die zu erwartenden Schäden übersteigen. In diesem Fall wird man vernünftigerweise von einer Risikominimierung absehen.

Bei der Festlegung der Strategie zur Risikominimierung sollte auch die von der Unternehmensleitung zu definierende Risikotoleranz des Unternehmens mit berücksichtigt werden.

Schritt 3: Langfristige Planung

Risikominimierung ist ein kontinuierlicher Prozess. Vor allem die Knappheit frei verfügbarer Ressourcen erfordert eine langfristige Planung. Risiken ändern sich mit der Zeit, und so müssen Strategien ständig kontrolliert und gegebenenfalls angepasst werden.

Virengefahr an sich ist ein konstantes Risiko, einzelne Viren ändern sich dagegen ständig. So routiniert ein Unternehmen also im Bereich Virenschutz auch sein mag ist trotzdem ständige Aufmerksamkeit nötig, um auf neue Viren reagieren zu können.

Jederzeit können neue Gefahren wie beispielweise durch Funknetzwerke und War Walkers auftreten und besonders die Expansion von Unternehmen in neue Märkte und neue Geschäftszweige oder auch die Übernahme anderer Unternehmen erhöhen das Grundrisiko signifikant.

DEN ÜBERBLICK BEHALTEN: RISIKOMINIMIERUNG UND DAS NETZWERK

Bei der Planung des Risikomanagements und der damit verbundenen IT-Planung muss stets die Funktionalität des kompletten Netzwerkes im Auge behalten werden.

Neben den Kosten müssen bei Überlegungen zur Risikominimierung auch andere Faktoren beachtet werden, wie etwa die Frage, ob Maßnahmen intern ergriffen werden sollen oder ob eventuell Outsourcing sinnvoller ist.

Oft wird diese Entscheidung aufgrund relativer Kosten, aufgrund von Verfügbarkeit oder speziellem Know-how oder aus firmenpolitischen Gründen getroffen. Dabei kann gerade hier das gesamte Risikoszenario grundlegend beeinflusst werden.

Risiken wie Datensicherheit und Datenwiederherstellung können an den Dienstleister weitergegeben werden. Allerdings geht das Unternehmen damit neue Risiken ein: Der Dienstleister kann möglicherweise SLAs (Service Level Agreements) nicht einhalten, oder vereinbarte SLAs entsprechen nicht den wirklichen Anforderungen des Unternehmens. Die Verlagerung von Risiken und die damit verbundene Kostensenkung werden neue Investitionen in die Kontrolle der Dienstleistung erfordern.

All dies erfordert eine durchdachte Planung, verbunden mit vorsichtiger Entscheidungsfindung, kann

aber letztlich zu einer deutlichen Risikominimierung zu vertretbaren Kosten führen.

Netzwerk-Monitoring ist ein weiteres, wichtiges Werkzeug zur Risikominimierung, das oft viel zu wenig genutzt wird. Diese Technologie wird meist nur in Zusammenhang mit dem Ausfall von Netzwerkkomponenten und dem Auffinden überlasteter Datenleitungen gesehen. Dabei bietet sie zahlreiche Möglichkeiten, bei den verschiedensten Bereichen des Risikomanagements mehr oder weniger direkt unterstützend eingesetzt zu werden.

Eines der Hauptrisiken sind Verzögerungen bei der Datenübermittlung, die durch erhöhten Netzwerkverkehr verursacht werden.

VoIP reagiert bekanntermaßen höchst sensibel auf diese Verzögerungen, so dass die Einführung von VoIP zumeist damit verbunden ist, dass VoIP-Packete eine höhere Priorisierung erhalten um nicht durch andere Daten beeinträchtigt zu werden.

Aber auch andere Anwendungen können mindestens genauso sensibel auf Verzögerungen bei der Datenübertragung reagieren. So kann beispielsweise die Verzögerung bei der Übermittlung von Transaktionsdaten Schäden bis hin zu Börsenverlusten für Unternehmen wie Fluglinien oder Finanzdienstleistern verursachen.

In modernen, hochgradig automatisierten Fertigungsbetrieben können Verzögerungen bei der Datenübermittlung ganze Produktionsanlagen ausbremsen und zu Produktionsausfällen führen. Der Verlust automatisch durchgeführter Bestellungen oder von Lieferterminen für JIT(just-in-time)-georderte Produktionen kann katastrophale Folgen haben. So kann bei vielen produzierenden Unternehmen eine professionelle Netzwerküberwachung einen ROI allein schon dadurch gewährleisten, dass wichtige Daten verzögerungsfrei ihr Ziel erreichen.

Konsequentes Monitoring kann auch dabei helfen, vermehrtes Datenaufkommen und die Ursachen dafür zu identifizieren. Die moderne Geschäftswelt wird immer mobiler und heute haben nicht mehr nur Manager Laptops und PDAs. Immer mehr Mitarbeiter nutzen mobile Geräte außerhalb geschützter Firmennetzwerke und erhöhen so das Risiko, dass Würmer, Trojaner und Co. vorbei an Firewalls in Unternehmen eingeschleust werden.

Oft besteht der erste Hinweis auf derartige Gefahren – ein infizierter Rechner versendet massenweise Spam oder startet denial-of-service-Attacken, ein Wurm verbreitet sich über das Netzwerk – aus Spitzen im Netzwerkverkehr, die von Monitoring-Tools entdeckt werden. Diese sind meist auch die ersten, die die Ursache des Problems identifizieren, so dass der Schädling ausgeschaltet werden kann.

Funknetzwerke und ihre speziellen Risiken

Immer häufiger zum Einsatz kommende Funknetzwerke bringen verschieden Risiken mit sich:

Die IT verliert einen großen Teil der Kontrolle darüber, welche Geräte mit dem Netzwerk verbunden sind. Dies bringt Risiken mit sich, die von Inkompatibilität zwischen Applikationen und angeschlossenen Geräten bis hin zu Zugriffen auf das

Netzwerk durch Besucher und nicht autorisierte Personen reichen.

Das Netzwerk reicht häufig über die physikalischen Wände des Firmensitzes hinaus und ist damit angreifbar für War Walker, die aus der Nachbarschaft oder von Parkplätzen und Gehwegen auf das Firmennetzwerk und möglicherweise auf interne Applikationen und Daten zugreifen.

Funkmodems können bekanntermaßen sehr einfach an ein Netzwerk angebunden werden. Netzwerkadministratoren entdecken häufig nicht autorisierte Funknetze, die plötzlich in Firmenbüros auftreten, nachdem Angestellte Funk-Modems an das Netzwerk in ihrem Büro angeschlossen haben. Oft machen sich diese Angestellten nicht die Mühe, die Zugangskontrollen dieses Modems zu aktivieren, und öffnen so eine potenzielle Lücke für Eindringlinge, die so die Firewall umgehen und in das Unternehmensnetzwerk eindringen oder Schädlinge einschleusen können.

Auch hier kann eine professionell eingesetzte Netzwerküberwachung der IT helfen, potenzielle Risiken, die durch Funknetzwerke zwangsläufig entstehen, zu entdecken und zu minimieren und so drahtlose Netzwerkumgebungen zu kontrollieren.

Eine lückenlose Überwachung des Aufkommens im Netzwerkverkehr ist heute besonders wichtig, da eine wesentliche Veränderung der Art und Menge der Geschäftsdaten stattgefunden hat. Textdateien, die noch bis vor Kurzem einen Großteil des professionellen Datenaufkommens ausmachten, sind mittlerweile durch eine ständig wachsende Menge von Grafiken und digitalen Audio- und Videodateien ersetzt worden. Damit kann ein Netzwerk, das noch für die Übermittlung von Textdateien konzipiert wurde, schnell an seine Grenzen stoßen. Es ist schwierig, dabei legitimen, geschäftlich bedingten Dateiversand von privater Unterhaltung oder gar diskriminierenden Inhalten zu unterscheiden.

Oft sind Seiten wie beispielsweise YouTube Verursacher von hohem Verkehr, allerdings werden legitim versendete Daten immer umfangreicher. So ersetzen beispielsweise zahlreiche Unternehmen Geschäftsreisen durch Telefon- und Videokonferenzen, häufig aus speziellen Konferenzräumen, oft aber auch vom individuellen Arbeitsplatz aus. Damit spart das Unternehmen viel Geld für Reisen, steigert die Produktivität und verringert gleichzeitig die Belastung seiner Angestellten durch den Wegfall von Reisezeiten und schont die Umwelt.

Das schnelle Anwachsen des Datenaufkommens, das durch stetig steigende Treibstoffkosten noch beschleunigt werden wird, vergrößert auch das Risiko von Engpässen und Leistungseinbrüchen im Netzwerk. Eine leistungsfähige Netzwerk-Monitoring-Lösung wie beispielsweise PRTG Network Monitor von Paessler kann neben der Überwachung in Echtzeit über die Auswertung von Langzeitdaten das Anwachsen des Datenaufkommens dokumentieren und analysieren und so dieses Risiko minimieren, indem es einerseits Verursacher von Verbrauchsspitzen identifiziert und andererseits eine bedarfsgerechte Planung beim Ausbau des Netzwerks ermöglicht.

Über die Paessler AG

Die Paessler AG mit Sitz in Nürnberg entwickelt Software für die Bereiche Netzwerküberwachung und Webserveranalyse seit 1997. Weltweit setzen mehr als 150.000 Administratoren, Webseitenbetreiber, Internet Service Provider und andere IT-Verantwortliche Paessler Software ein. Freeware- und Testversionen aller Produkte können unter www.de.paessler.com heruntergeladen werden.

RISIKOMANAGEMENT MIT PAESSLER SOFTWARE

Die Paessler AG ist auf Netzwerk-Überwachungs-Software spezialisiert und bietet mit PRTG Network Monitor eine umfassende Lösung zum Verfügbarkeits- und Bandbreiten-Monitoring für Netzwerke aller Größen an, die sich durch einfache Installation und Bedienbarkeit, hohe Leistungsfähigkeit und ein umfassendes und praxisnahes Featureset auszeichnet.

Damit ermöglicht PRTG Network Monitor IT-Administratoren die ständige Kontrolle ihres gesamten Netzwerks in Echtzeit ebenso wie das Erkennen langfristiger Auslastungstrends mittels historischer Daten. Das PRTG AddOn „NetFlow Sensor“ ermöglicht die Auswertung des NetFlow-Protokolls und damit die umfassende Überwachung von Cisco Hardware, die dieses Protokoll unterstützt. (www.de.paessler.com/prtg7)

In Ergänzung zu PRTG bietet Paessler mit dem SNMP Helper die Möglichkeit, über WMI zahllose Informationen zu Windows-Systemen zu sammeln und zu analysieren. (www.de.paessler.com/snmphelper)

Webserver Stress Tool ist eine Testsoftware für HTTP-Server (Webserver), die versteckte Performanzprobleme von Webservern bzw. Webapplikationen, die unter großer Last auftreten, aufdeckt. Durch Simulation von hunderten oder tausenden Benutzern, die gleichzeitig HTTP-Anfragen an einen Server senden, testet Webserver Stress Tool das Verhalten von Webservern unter normaler und außerordentlicher Last. (www.de.paessler.com/webstress)

Alle Paessler-Lösungen sind in verschiedenen Versionen, als Freeware-Edition mit eingeschränktem Leistungsumfang und als 30-Tage-Testversion erhältlich.

RESÜMEE

Es gibt keine absolute Garantie. Das Leben ist voller Risiken, und ein gewisses Maß an Risiken muss von jedem Unternehmen akzeptiert werden. Risikomanagement kann nicht garantieren, dass keine Risiken mehr auftreten – auch das sicherste Szenario wird immer wieder vor Probleme gestellt werden.

Das Ziel eines strategischen Risikomanagements muss sein, die Gefahr auf ein akzeptables Niveau zu reduzieren, das einerseits finanzierbar und anderseits nicht mehr existenzbedrohend ist. Sobald die IT das erreicht hat, kann sie ihr Risikomanagement als erfolgreich betrachten.

Paessler Software

PRTG Network Monitor
Verfügbarkeits- und Bandbreitenüberwachung in Netzwerken
www.de.paessler.com/prtg

SNMP Helper
Überwachung von Windows-System-Parametern
www.de.paessler.com/snmphelper

Webserver Stress Tool
Webserver Performance-, Last- und Stress-Test
www.de.paessler.com/webstres

PAESSLER®
the network monitoring company

Paessler AG • Burgschmietstraße 10
90419 Nürnberg • Deutschland
www.de.paessler.com • info@paessler.com