

Der Weg zum professionellen IT-Risk-Management (Teil 1)

Klassifizierung der Risiken in der IT

Das Ziel eines professionellen Risikomanagements ist, die wirklich kritischen Risiken zu identifizieren, um sie im nächsten Schritt auf ein Minimum zu reduzieren. Mit einem bestimmten Restrisiko müssen sich Unternehmen jedoch abfinden, einen hundertprozentigen Ausschluss gibt es nicht.

So können gerade kleinere und mittelständische Unternehmen nicht unbegrenzt Ressourcen für diesen Bereich einsetzen. Oft reagieren sie nur auf akut anliegende Probleme, wie beispielsweise eine Virus-Attacke; mit dem Ergebnis, dass eine entsprechende Anti-Viren-Software installiert wird. Ein geplanter und übergreifender Ansatz steht nur selten dahinter. Auf dem Weg zu einem konzeptionellen und erfolgreichen IT-Risk-Management sind drei Bereiche zu beachten. Im ersten Schritt ist es wichtig, sich mit den verschiedenen Risikoklassen in der IT zu befassen:

Technologie-Risiken

Dabei handelt es sich um oft schon bekannte IT-Risiken wie mögliche Equipment-Ausfälle, Virus- und Wurmattacken aus dem Netz sowie Denial-of-Service-Attacken. Unberechtigter Zugriff und Angriffe über das drahtlose Netzwerk von außen zählen ebenfalls dazu. Viele Gegenmaßnahmen zur Bekämpfung dieser potenziellen Probleme basieren wiederum auch auf Technologie, doch sollte dies die Verantwortlichen nicht davon entbinden, eine stringente Firmenpolitik als wichtigen Bestandteil in das Gesamtkonzept zu integrieren. Beispielsweise müssen mobile Geräte durch einheitliche Vorgaben auf das Schärfste durch Firewall- und Antivirus-Überprüfung abgesichert werden. Außerdem sollten Mitarbeiter dazu angehalten werden, keine eigenen unkontrollierten und oft ungeschützten Wifi-Nodes zu installieren. Eine Schlüsselrolle kann hierbei ein konsequentes Netzwerk-Monitoring mit professionellen Tools wie beispielweise

PRTG von Paessler bilden, das auffällige Änderungen im Netzwerk sofort registriert und meldet.

Rechtliche und personelle Risiken

Um solche zu vermeiden, ist unbedingt die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien hinsichtlich der juristischen Offenlegungspflichten erforderlich. Dies gilt für E-Mails, in Zivilprozes-

sen, bei Mitarbeitern, die rechtlich bedenkliches Material aus dem Internet herunterladen, und in potenziellen Sabotage- und Spionagefällen durch Mitarbeiter. Dieser Art von Bedrohungen kann wesentlich schwieriger begegnet werden, da es keine übergreifende Technologie gibt, die hierfür eine allumfassende Lösung liefert. Eine klare Personalpolitik und ein gutes Management sind die Schlüssel, die diese Risiken deutlich senken können. Eine weitere Hilfestellung kann auch hier ein konsequentes Netzwerk-Monitoring mit Tools wie PRTG leisten, das über die Klassifizierung von Protokollen und IP-Adressen die genaue Analyse und Zuweisung des Netzwerkverkehrs ermöglicht.

Von der Natur und durch Menschen verursachte Katastrophen

Überflutungen, Erdbeben, große Stürme und ähnliche Vorkommnisse bringen Verwüstungen mit sich. Strategien zu entwickeln, die es ermöglichen, mit derartigen Gefahren richtig umzugehen, ist eine der schwierigsten Aufgaben im Risikomanagement. Verschiedene Strategien sind zu unterschiedlichen Preisen und mit unterschiedlichen Schutzstufen verfügbar. Sie sollten jedoch sorgfältig auf den Gesamtkontext der jeweiligen geschäftlichen Situation abgestimmt sein. Katastrophenmanagement sollte zuerst mit gesundem Menschenverstand angegangen werden. In der heute zunehmend vernetzten Welt sind auch relativ kleine Unternehmen in der Lage, ihre Datenzentren außerhalb gefährdeter Gebiete zu betreiben, zudem in einem sicheren Gebäude (eventuell gemeinsam mit anderen Firmen). Eine weitere Möglichkeit ist es, mit Outsourcing-Spezialisten oder Service-Providern (SaaS) zu arbeiten, die ein Höchstmaß an Sicherheit bieten können.

In der Ausgabe vom 27. August 2008 stellen wir einen 3-Stufen-Plan zur Risikominderung vor.

Checkliste

Verfahren, um Netzwerkprobleme zu diagnostizieren und aufzuspüren

- Führen Sie ein kontinuierliches Monitoring von Netzwerk und Servern ein
- Verfolgen Sie wichtige Performance-Indikatoren und Trends
- Planen und teilen Sie gezielt Bandbreitenauslastung ein
- Achten Sie auf Sicherheitslücken, die Traffic und Last beeinflussen
- Behalten Sie kritische Anwendungen, die Bandbreite binden, permanent im Auge
- Reduzieren und verhindern Sie unerwünschten Traffic



Paessler AG
Burgschmietstraße 10
D-90419 Nürnberg

Tel.: +49 (911) 7 39 90 30
Fax: +49 (911) 7 39 90 31
E-Mail: info@paessler.com
URL: www.de.paessler.com

Ansprechpartner: Christian Twardawa