



**Verantwortung
& Haftung
für IT-Sicherheit**



**IT-Standorte,
optimal und sicher
geplant!**



proRZ

professioneller
Rechenzentrumsbau

Industriestraße 41
D-57518 Betzdorf

Phone: +49 (0) 2741 9321 - 0
Fax: +49 (0) 2741 9321 - 111
info@proRZ.de · www.proRZ.de



proRZ

professioneller
Rechenzentrumsbau



Thomas Federrath
Geschäftsführer proRZ Rechenzentrum GmbH

Vorwort

In vielen Fällen bedeutet IT-Standortoptimierung Konzentration von zum Teil weltweiten Anwendungen auf immer kleinerer Fläche. Damit steigen die Risiken, dass bei einem Ausfall durch z.B. nicht richtig konzipierte Klimaanlage z.B. auch die Produktion in Osteuropa oder China zum Erliegen kommt. Eine sorgfältige Analyse der IT-Infrastruktur gehört somit zu den Basis- Voraussetzungen für eine gute RZ- und Serverraumplanung. Leider sieht es in der Praxis oftmals anders aus und viele Unternehmen nehmen bewusst oder unbewusst erhebliche Sicherheitslücken in ihrer IT-Standortpolitik in Kauf. Dabei ist ein Ausfall der IT neben dem unmittelbaren Schaden auch immer häufiger

mit weiteren Schäden wie kundenseitigen Regressansprüchen, Unterbrechung von Betriebsabläufen, Imageschäden bis hin zu haftungsrechtlichen Folgen für die Verantwortlichen verbunden. Doch wie findet ein Unternehmen das richtige Maß für seine IT-Standortpolitik und welche Irrtümer gilt es aufzudecken? Das wollen wir Ihnen in dem nachfolgenden Kapitel näher erläutern und Ihnen konkrete Tipps für die Praxis geben. Gerne stehen wir Ihnen auch für ein unverbindliches Erstberatungsgespräch zur Verfügung und freuen uns über Ihre Kontaktaufnahme.



IT-Sicherheit- ganzheitlich betrachtet

Grundsätzlich bedeutet IT-Sicherheit mehr als logische und technische Sicherheit. Zusätzlich zu den bekannten Sicherheitsmaßnahmen wie beispielsweise Firewalls, Virenschutz oder Speicherkonzepte gibt es noch ein weites Feld an Maßnahmen, welche die IT und deren Standort absichern. Alle Strategien bestimmen unmittelbar die Ausfallsicherheit – angefangen vom Grundschutz bis hin zur Hochverfügbarkeit. Die zusätzlich erforderliche Absicherung des physikalischen Umfeldes lässt sich im Rahmen einer wirtschaftlichen IT-Optimierung innerhalb kurzer Zeit analysieren und umsetzen. Unternehmens- und IT-Verantwortliche sollten deshalb nach Möglichkeit ein ganzheitliches Augenmerk auf folgende, beeinflussende Kriterien richten:

Risiko: Brand/Feuer

Fakt ist, dass nur etwa 20% aller Brände im direkten Umfeld von IT-Standorten, bzw. im Rechenzentrum, bzw. Serverraum selbst, entstehen. 80%, also die Mehrheit aller Brände,

entstehen außerhalb. Die Folgen sind: IT-Standorte müssen gegenüber Löschwasser, Rauchgasen und Hitze geschützt werden. Die Lösung könnte ein den kundenseitigen Anforderungen angepasstes Mini DataCenter, Serverraum oder in größeren Dimensionen ein Rechenzentrum sein, der/das in einen bestehenden Raum integriert



wird. Eine weitere Alternative stellt die „Ertüchtigung“ des bestehenden physikalischen Umfeldes darstellen. Zu einer „artgerechten“ Server-/IT-Haltung gehört es z.B., eine

Brandfrühsterkennung zu implementieren. Diese erkennt Brände, bevor sie Schäden anrichten. Ein Rohrsystem saugt ständig Luft aus dem Serverraum und kontrolliert, ob spezielle Aerosole in der Raumluft auftreten. Diese Gase stammen von den Weichmachern in den Kabeln, die vor der Überhitzung ausströmen. Nicht zu unterschätzen ist dann die weitere Alarmablaufplanung, um situationsbezogen auf die Warnungen zu reagieren.



Risikofaktor Staub

Die feinen Partikel sind der natürliche Feind der Elektronik. Die Lebensdauer von Lüftern und der elektronischen Bauteile reduziert sich enorm. An IT-Standorten, die physikalisch unzureichend gesichert sind, entsteht immer wieder Staub, z.B. bedingt durch handwerkliche Aktivitäten. Die professionelle Absicherung eines IT-Standortes sollte immer staubfrei realisiert werden. Da dieses „Handwerk“ nur wenige Unternehmen verstehen, ist es ratsam, sich entsprechende Referenzen aufzeigen zu lassen.

Risikofaktor Zugang/Dichtigkeit

Der Zugang zu einem Serverraum zählt zu einem der sensibelsten Bereiche. So sollte beispielsweise die Türe speziellen Anforderungen gegen Brand und Rauch-Gasdichtigkeit genügen. Hier muss



insbesondere auf die regelmäßige Wartung

geachtet werden. Darüber hinaus erhöht es die Sicherheit, den Zugang exakt zu regeln und in einer Datenbank jedes Betreten zu protokollieren. Ist ausreichend Platz vorhanden, so sollte die Klima- und Elektrotechnik von den laufenden Servern räumlich getrennt werden, um bei Servicebedarf einen getrennten Zugang zu sichern.

Risikofaktor Klimatisierung

Der Einsatz moderner Hochleistungsserver wie z.B. Blade-Server Technologien erzeugt zunächst ein Plus an Leistung und ein Weniger an Wartung. Was vielfach aber unterschätzt wird, dass die - wie in vielen mittelständischen Unternehmen-gewachsene Struktur eine Überlastung der Klimatisierung und Elektroversorgung zur Folge haben kann. Im Normalfall wird dann der Kontakt zu einem Klimahersteller gesucht und ein Angebot für eine leistungsstärkere Anlage unterbreitet. Meist werden dann Facility- Management oder ein externer Elektriker beauftragt, die Arbeiten umzusetzen. Dass oftmals keiner der beiden Seiten Experte für die Kompatibilität der eingesetzten Lösungen ist, wird vergessen. Wirtschaftlicher ist es, einen Experten wie die proRZ mit der



Optimierung zu beauftragen. Dabei führen clevere und moderne Energie- und Klimakonzepte zu nachweisbaren Einsparpotentialen von bis zu 30% und reduzieren das Restrisiko.

Risikofaktor Energieversorgung

Die Absicherung der Energieversorgung ist ein wichtiges Thema für IT-Standortpolitik. Eine Unterbrechungsfreie Stromversorgung (USV), die Einspeisung eines Notstromaggregats und auch die Absicherung der Kabeltrassen gegen Brände lassen sich bei professioneller Planung problemlos implementieren. Redundante Energiekonzepte runden eine professionell realisierte IT-Standortoptimierung ab.

EMV-Schutz

Die Elektro-Magnetische Verträglichkeit (EMV) wird in verschiedenen Normen geregelt. Optimale IT-Sicherheitslösungen können auf Wunsch mit einer besonderen Abschirmung ausgestattet werden, so dass keine Strahlung den Serverraum oder das Rechenzentrum verlässt oder eindringt.

Kabel-Management

Energie- und Datenkabel werden sauber auf Kabelpritschen verlegt. Der Anwender erhält dadurch eine verbesserte Sicherheit, da er sofort weiß, welches Kabel wohin gehört. Außerdem verkürzen sich die Reparaturzeiten, wenn etwa Serverschränke umgeräumt werden.

Risikofaktor Hochwasser, Erdbeben, Vandalismus, Terroristische Anschläge

Gute Sicherheitslösungen lassen sich gegen Erdbeben, Hochwasser und Vandalismus absichern. Auch die Absicherung gegen gewaltsame Einwirkungen von außen lässt sich durchführen.

Risikofaktor Mitarbeiter

Neben den immer häufiger und gefährlicher werdenden Angriffen von außen, gewinnt auch der Schutz vor internen Attacken an Bedeutung. Obwohl externe Angriffe auf die IT-Struktur



und damit auf ein Unternehmen wesentlich höhere öffentliche Aufmerksamkeit erregen, sind interne Angriffe leider an der Tagesordnung. Das bestätigen auch offizielle Studien, die den Anteil interner Angriffe auf die Unternehmens- IT auf bis zu 80 Prozent schätzen. Mal schleusen Mitarbeiter Spionageprogramme ins interne Netzwerk ein oder entwenden heimlich Daten zu neuesten Entwicklungen. Im Rahmen des Schutzes der unternehmenseigenen IT gegen interne und externe Angriffe sollten Unternehmen auch Maßnahmen zur Sicherheit in Kommunikationsnetzwerken treffen.

Zukunftsfähigkeit

Für Unternehmen wird es immer schwieriger, langfristig zu planen. So fällt es schwer, einen überraschenden IT-Boom oder Technologiewechsel abzubilden. Auch das Gegenteil, der Abbau, das Zusammenlegen oder der Umbau von Kapazitäten ist mit herkömmlicher IT-Standortpolitik nur schwierig zu realisieren. Darüber hinaus bindet die allzu großzügige Planung eines IT-Standortes viel Kapital. Doch wie sehen die Alternativen dazu aus?

Flexibilität/Skalierbarkeit

Optimale Lösungen bieten Flexibilität und Investitionssicherheit. Durch die intelligente Nutzung bestehender Gebäude- Produktions- oder Büroflächen muss nicht immer neu gebaut werden. Im Gegenteil, wirtschaftliche Sicherheitslösungen lassen sich problemlos und binnen kurzer Zeit in die vorhandene, auf den ersten Blick nicht geeignete Infrastruktur integrieren, bzw. erweitern. Aus diesem Grund ist eine an die aktuellen Bedürfnisse anpassbare Raumstruktur das beste Mittel gegen steigende Kosten.

Standortwechsel mit dem proRZ Umzugsservice

Zur Komplettierung des Leistungsspektrums gehört auch die Umzugsplanung von IT-Standorten und individuelle Netzwerkplanung. Diese Bereiche umfassen sowohl die Aufstellung der Hardware im Serverraum oder in einem Rechenzentrum, die Planung der optimalen Energie- und Kälteversorgung der Einzelkomponenten sowie der Netzwerke. Wir unterstützen Sie mit Partnern bei der Planung und Durchführung eines Umzugs der IT-Hardware auf die neu geschaffenen Flächen.



Schneller Betriebsbereit

Sie haben während der Realisierung eines Projektes nur einen Ansprechpartner. Somit können Sie sich ganz auf Ihr tägliches Geschäft konzentrieren. Bei der Umsetzung der Infrastruktur richtet sich der Spezialist nach den kundenspezifischen Geschäftszeiten und koordiniert die unterschiedlichen Gewerke danach, nicht umgekehrt! Viele der realisierten IT-Projekte werden deshalb am Wochenende und am Abend durchgeführt. Eine umfassende planungs- und ausführungsbegleitende Betreuung unterstützt Sie in allen Fragen der Realisierung während der gesamten Projektdauer bis zur Abnahme. In der Ausführungsplanung werden die Pflichtenheftvorgaben mit den erforderlichen Details präzisiert, wobei die spezielle überbetriebliche Erfahrung aus Planung und Beratung sowie der Ökonomisierung von Sicherheit zum Tragen kommt.

- ◆ RZ-Konzepte und Planungen
- ◆ Sicherheitsanalysen
- ◆ Durchführung der Baumaßnahmen anhand der technischen Planung
- ◆ Bauleitung inkl. Überwachung der Umsetzungsmaßnahmen
- ◆ Generalunternehmerschaft
- ◆ Schlüsselfertige Übergabe des ausgeführten Projektes an den Kunden

Aller Anfang ist leicht

Um die Vorort-Situation zu erfassen, wird als erstes die Ist-Situation erfasst und die baulichen Möglichkeiten überprüft. Dann erfolgt ein detaillierter Planungsvorschlag unter Berücksichtigung wirtschaftlicher Aspekte. Ein ganzheitliches und bezahlbares Beratungspaket gibt entsprechende Planungssicherheit. Erfahrene Projektleiter zeigen Ihnen die Möglichkeiten auf, wie IT rundum sicherer gemacht werden kann.

Ganzheitliche Beratung

Die ganzheitliche Beratung ist kein leeres Schlagwort: Risikoanalyse von DV-Systemen sowie die Erfassung und Bewertung der Bauausführung oder der verschiedenen Standorte gehören zum Programm. Die Fachplanung sowie ein Pflichtenheft sind ebenfalls Bestandteil eines kundenfreundlichen Angebotes. Darüber hinaus hat der Kunde die Zusicherung, dass er eine herstellerneutrale Bewertung seiner Lösung erhält.



Umfassendes Servicekonzept

Ob klein, mittel oder Konzernstruktur- die Anforderungen an die Verfügbarkeit der IT und deren Standort steigen stetig. Neben der Leistungsfähigkeit von IT und Telekommunikation nimmt auch der lückenlose Service, bzw. die Wartung dieser Bereiche zu. Ein Ausfall der Verfügbarkeit bedeutet in der Regel für alle Unternehmen inzwischen Handlungsunfähigkeit. Langjährige Praxiserfahrung und intensive Diskussionen mit Kunden veranlassten proRZ zur Entwicklung eines leistungsfähigen und individuell anpassbaren Servicekonzepts. Das Portfolio umfasst drei aufeinander abgestimmte Levels, die neben Wartung und Service u.a. nachfolgender Komponenten

- Klimatisierung
- Brandmeldelöschanlage
- Brandfrühesterkennung
- USV
- Netzersatzanlage

gleichermaßen auch das physikalische IT-Umfeld mitsamt seiner Energie- und Stromzufuhr abdeckt.

Folgende Leistungen können je nach der angestrebten Zielsetzung vereinbart werden:

- Kompletter technischer Kundendienst für alle installierten Gewerke (Service Level Agreements, 24h-Hotline, Monitoring)
- Erarbeitung eines Sicherheitskonzeptes für den gesamten IT-Prozess
- Zertifizierung der Komplettlösung (z.B. nach TÜV-Standards)
- Finanzierungslösung für die gesamte physikalische Infrastruktur

Remote Management

Über ein spezielles Controlling-Tool lassen sich alle Funktionen im Schutzraum extern steuern und kontrollieren. Sobald ein Alarm auftritt, wird die richtige Aktion veranlasst. Beispielsweise kann ein ständig besetztes Call-Center eine Kurznachricht (SMS) an den Administrator senden oder Aktionen gemäß Alarmablaufplan anstoßen.



Besseres Rating durch Versicherungen & Finanzinstitute

Durch nachweisbare Absicherung der physikalischen IT-Infrastruktur stufen Versicherer das Risikopotential wesentlich geringer als vorher ein und sind eher bereit, Versicherungsprämien zu reduzieren. Auch der Verpflichtung der Finanzinstitute und Wirtschaftsprüfer, kreditsuchende Unternehmen auf eine sichere IT zu prüfen, wird mit realisierten IT-Sicherheitsmaßnahmen und einer vorgeschalteten Analyse der Ist-Situation Genüge getan.

