

# Behörden Spiegel

Unabhängige Zeitung für den Öffentlichen Dienst

**Sonderdruck**

Nr. II / 26. Jahrgang

Berlin und Bonn / Februar 2010

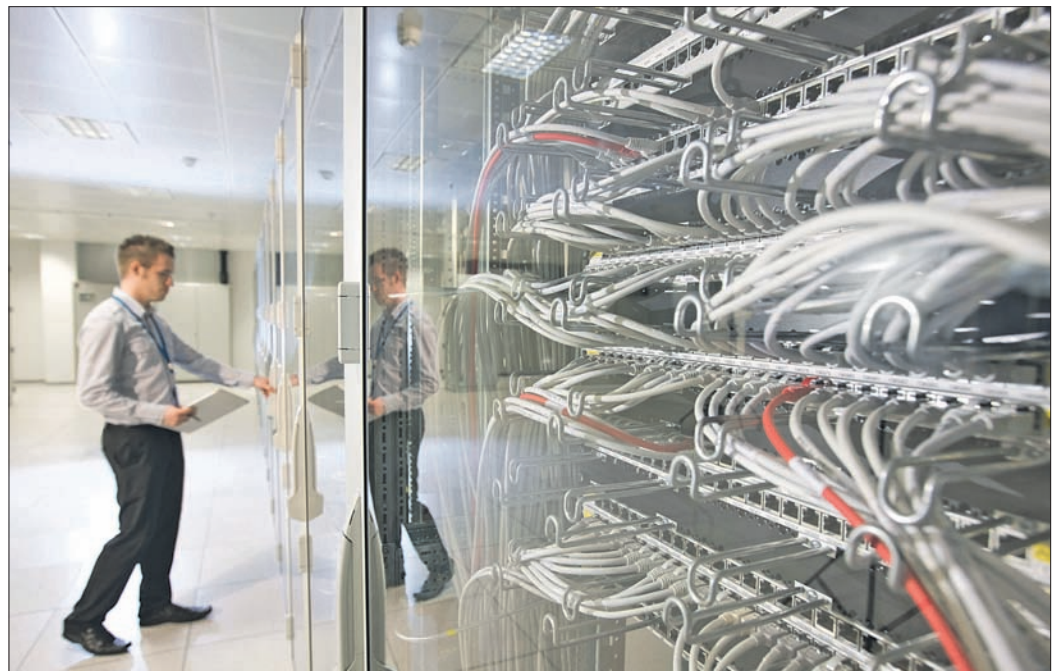
www.behoerderspiegel.de

## Fort Knox 2.0

Rundum-Schutz in Rechenzentren

**(BS) In vielen Bereichen des öffentlichen Sektors gehören die Verarbeitung und Archivierung von personenbezogenen oder sicherheitskritischen Daten zum Tagesgeschäft. Darunter fallen Daten von Bürgern und Unternehmen, von Behörden und Organisationen mit Sicherheitsaufgaben und Daten über die eigenen Mitarbeiter. Im Zuge der Verwaltungsmodernisierung werden immer mehr Informationen und Dokumente digital erfasst, verarbeitet, weitergeleitet und gespeichert.**

In digitaler Form benötigen Daten wenig Platz, sie wiegen nichts und sind prinzipiell von überall her zugänglich. Das ist effizient, schafft aber auch neue Gefahren. Daten können beschädigt werden oder verloren gehen, vorübergehend nicht abrufbar sein, oder sie können in falsche Hände geraten. Wirksame Präventionsmaßnahmen müssen die gesamte Prozesskette des E-Governments abdecken, von der Erfassung bis zur Ablage. Dabei spielt es zunächst keine Rolle, ob sich Daten beispielsweise auf einem Büro-PC befinden oder in einem Rechenzentrum.



Bei den Mitarbeitern eines Rechenzentrums spielt neben den hohen fachlichen Fähigkeiten vor allem auch die persönliche Integrität eine Rolle.

Foto: BS/T-Systems

### Standortwahl und bauliche Sicherheit

Die physikalische Sicherheit eines Rechenzentrums beginnt mit der Standortwahl. Ideal ist ein Standort mit guter Verkehrsanbindung, stabiler

Energie- und Wasserversorgung sowie guter Kanalisation, und zwar in Regionen, wo Natur- und andere Katastrophen unwahrscheinlich sind. Gebäude müssen Hagel und Sturm ebenso standhalten

wie Bomben oder Feuer. Von einer werblichen Außenkennzeichnung ist abzuraten. Sie kann auf potenzielle Angreifer wie eine Einladung wirken. Zu den Sicherheitsvorkehrungen auf dem Gelände

gehören ein nach allen Seiten gesicherter Zaun und ein Schleusenverfahren für Durchfahrten und Warenanahme. Hinzu kommt eine umfassende Kamera-Überwachung von Gelände und Rä-

umlichkeiten nebst einer datenschutzkonformen Aufbewahrung der Aufzeichnungen.

Ein wesentlicher Bestandteil jedes Rechenzentrums ist die Vereinzelungsanlage. Hier sorgen beispielsweise steuerbare Drehkreuze dafür, dass zur gleichen Zeit immer nur eine Person das Rechenzentrum betreten kann. Jeder einzelne Besucher oder Mitarbeiter muss sich einzeln einloggen und registrieren lassen. Ohne Ausweis oder Mitarbeitercodierung erhält niemand Zutritt. Zu besonders sensiblen Bereichen ist der Zugang nur mit zusätzlichen Zutrittskarten oder in Begleitung möglich. Zutritt zu allen Räumlichkeiten haben grundsätzlich nur Sicherheitsmitarbeiter, und auch sie werden von Kameras überwacht.

Um die permanente Verfügbarkeit nicht nur der IT, sondern auch der verschiedenen Sicherheitssysteme zu gewährleisten, muss die Stromversorgung extrem krisenfest sein. Rechenzentren von T-Systems erhalten ihren Strom über eine oder mehrere Einspeisungen von lokalen Stadtwerken, bei einem Ausfall wird weiterschaltet. Hinzu kommen zwei Batterieaggregate und ein Dieselaggregat. Wenn die normalen Stromeinspeisungen gleichzeitig ausfallen, springen Dieselgeneratoren an und versorgen das Rechenzentrum einschließlich Klimatechnik und Kühlung, bis die normale Einspeisung wieder funktioniert.

Extrem hohe Ausfallsicherheit schafft ein zweites Rechenzentrum, das als "Zwil-

ling" soft- und hardwaretechnisch dem Hauptrechenzentrum gleicht, sich aber ganz woanders befindet. Beide Rechenzentren sind über zahlreiche Leitungen miteinander verbunden, über welche die Daten des Hauptrechenzentrums permanent gespiegelt werden. Im Falle einer größeren Störung kann der "Zwilling" dann sofort die Komplettlast übernehmen und den Betrieb reibungslos weiterführen.

### **Personal: Integre Fachleute gefragt**

Bei den Mitarbeitern eines Rechenzentrums zählen neben hohen fachlichen Fähigkeiten vor allem die persönliche Integrität. Zum Einsatz kommen speziell geschulte Teams für Betrieb, lokales Netz und Installationsaufgaben und können im Störfall rund um die Uhr schnell handeln. Je nach Tätigkeit sind persönliche Sicherheitsüberprüfungen oder das Vorlegen von Führungszeugnissen zwingend.

Spezielle Vorschriften gelten für Mitarbeiter, die im Rahmen ihrer Aufgaben auf Kundendaten zugreifen müssen. Individuell definierte Berechtigungskonzepte regeln den Zugriff auf Daten, der verbindliche Sicherheitsrahmen richtet sich nach den Wünschen und Vorgaben des Kunden. Sowohl Administratoren als auch Endanwender dürfen ausschließlich Tätigkeiten auf Basis ihrer jeweiligen Berechtigungen durchführen, die sie mittels Benutzererkennung und

Passwort, Smartcard, Biometrie-Lösungen, SIM-Card vom Handy oder einer Kombination aus verschiedenen Authentisierungsverfahren nachweisen müssen. Vorschriften zur Weitergabekontrolle sowie zur unwiderruflichen Vernichtung von Daten und Datenträgern sind strikt einzuhalten.

### **Sicherheit von IT und Netzen**

"Never change a running system" – diese Informatikerweisheit darf als überholt gelten. Kleinere Software-Updates (Patches) an Betriebssystemen und Anwendungen sind heute an der Tagesordnung. Oft schließen sie neu entdeckte Sicherheitslücken, manchmal führen sie aber auch zu neuen Problemen. Bei T-Systems hat ein Computer Emergency Response Team (CERT) verschiedene qualitätssichernde Verfahren entwickelt, um Patches zu überprüfen, bevor sie aufgespielt und verteilt werden. Darüber hinaus kümmert sich das Team um die Bekämpfung und Prävention von kriminellen Aktivitäten. Das Spektrum reicht von der Abwehr von Distributed Denial of Service-Attacken und anderen Angriffen bis zur Identifizierung von Spionen und Daten- oder Identitätsdieben.

Daten müssen nicht nur sicher im Rechenzentrum liegen, sie müssen auch sicher und zuverlässig zum Kunden und zurück gelangen. Deshalb müssen Kunden über Weitverkehrsnetze sicher, authentifiziert und verschlüsselt mit

dem Rechenzentrum kommunizieren können. Angriffe und unerlaubte Zugriffe auf solchen Datenverkehr lassen sich mit verschiedenen Technologien wie Intrusion-Detection-Systemen erkennen und abwehren. Eine garantierte WAN-Übertragungsqualität inklusive Priorisierung, Service Level Agreements und eine Ende-zu-Ende-Verschlüsselung sollten daher im Angebot eines Rechenzentrums nicht fehlen.

Um festzustellen, ob die eigenen Konzepte und Maßnahmen auch wirksam sind, führt kein Weg an einer objektiven Beurteilung durch Dritte vorbei. Deshalb lässt T-Systems seine Rechenzentren nach ISO/EC 27001 zertifizieren. Kern dieser Zertifizierung ist der Nachweis eines Information Security Management Systems (ISMS), das die Sicherheits- und Risikoprozesse und ein umfassendes Security Framework normgerecht regelt. Dazu zählen physikalische Sicherheit, Zugangskontrolle, Datensicherheit, Umgebungschutz, Logging und Monitoring. Zudem prüfen die Auditoren Netze, Plattformen und Betriebssysteme, die Netzwerk-Sicherheitsarchitektur und Disaster Recovery. Nicht zuletzt geht auch der Faktor Mensch in die Zertifizierung ein: Auswahl, Schulung, Fähigkeiten und Sensibilität von Mitarbeitern werden ebenso unter die Lupe genommen, damit rundum alles getan ist, um ein Maximum an Datenschutz und Datensicherheit zu gewährleisten.