

IT-SICHERHEIT

Optimaler Schutz

Wasser oder Wasserdampf fördern, noch dazu in Verbindung mit elektrischem Strom die Korrosion. Nur jene Wasserversorgung soll in das Rechenzentrum gelangen, die unbedingt nötig ist, etwa zur Kühlung der Rechner. Klimaanlage sollten außerhalb des Rechnerraums sein. Über dem Rechenzentrum sind Nasszellen zu vermeiden. Wasser kann als Löschwasser von oben kommen. Direkte Kabeldurchlässe nach oben können kaum ausreichend abgedichtet werden. Wandhydranten sollten plombiert sein, die Hydrantentüren durch Öffnungskontakte überwacht werden. Versteckte Bodeneinläufe, Fassadenöffnungen oder Gefällebildung lassen Wasser abfließen.

Gegen Sabotage gesichert sollte auch die Klimaanlage sein. Luft, die zur Raum- und Gerätekühlung über die Klimaanlage vom Doppelboden durch die Racks geleitet und an der Decke wieder abgesaugt wird, bildet im oberen Bereich Wirbel, in denen Wärmesterne entstehen. Zwei Drittel der Systemausfälle geschehen im oberen Drittel der Schränke. „Mit Rechenprogrammen können derartige Strömungs- und Wärmeverhältnisse in 3-D-Modellen simuliert werden“, erläuterte Dipl. Phys. Markus Offermann. Zwar ist die Rechenzeit hoch, erspart aber umfangreiche und technisch aufwändige Messverfahren. Die Wirksamkeit von Einbauten zur Optimierung der Luftströmung kann im Rechenmodell erprobt werden.

Foto: K. Heckisch



Rainer von zur Mühlen: „Die Sicherheitsplanung muss so früh wie möglich einsetzen.“

Sichere Rechenzentren

Die Sicherheit und Höchstverfügbarkeit von Serverparks, Rechenzentren und IT-Räumen waren die Schwerpunktthemen einer Fachtagung in Berlin.

Welche Gefahren sind allgemein beim Betrieb von Anlagen der Informations- und Kommunikations-Technologie zu bedenken? Antworten auf diese Frage gab es bei der dreitägigen Fachtagung der *Simedia GmbH* Ende September 2005 in Berlin. Bei der Abhängigkeit von der Verfügbarkeit dieser Technik lohnt es sich, die eigenen Anlagen zu überdenken. „Die Sicherheitsplanung muss bereits zum frühestmöglichen Zeitpunkt einsetzen“, forderte Dkfm. Rainer von zur Mühlen zu Beginn der Tagung. „Gefahren dürfen nicht isoliert betrachtet werden. Das Erkennen von Zusammenhängen ist eine der vorrangigen Rollen des Sicherheitsexperten.“

Vom strategischen Ansatz her stehen Eintrittswahrscheinlichkeit und Schadenshöhe zueinander in einem in Grenzen beeinflussbaren, wechselseitigen Verhältnis. Der Diebstahl von Büromaterial besonders in der Zeit um

Schulbeginn ist zwar häufig, aber von der Schadenshöhe her nicht so gravierend wie etwa ein das Unternehmen treffendes Jahrhundert-Hochwasser.

Die Hochwasserkatastrophe des Jahres 2002 hat es gezeigt: Schon der Standort muss für ein Rechenzentrum geeignet sein, und auch die Nachbarschaft. Bestehen dort Brandgefahren (Reifenlager)? Drohen Gefahrgutunfälle? Muss mit dem Austritt chemischer Schadstoffe gerechnet werden (Chemiebetrieb)? In Kleingartenanlagen werden mitunter Abfälle verbrannt – schaltet die Klimaanlage in solchen Fällen auf Umluft, um nicht Rauchpartikel einzusaugen?

Das Eindringen von Rauch in ein Rechenzentrum muss wegen der Korrosionswirkung verhindert werden. Ritzen und Fugen bei Wandabschlüssen können erkannt werden, wenn mit einem Handscheinwerfer in den abgedunkelten Raum zu leuch-

ten versucht wird. Kabeldurchlässe müssen geschottet werden. Da Türen von Aufzugschächten einen Sicherheitsspielraum aufweisen müssen, wirken Aufzugschächte wie Rauchtransporteure. Abgehängte Decken können Schwelbrände des Isoliermaterials und dabei entstehende zündfähige Gasgemische weiterleiten. Flackernde Leuchtstoffröhren oder solche, deren Elektroden dauernd glühen, stellen wegen der Wärmeentwicklung eine Zünd- und Brandquelle dar.

„Rechenzentren verqualmen normgerecht“: Damit zeigt Rainer von zur Mühlen auf, dass weniger der offene Brand in einem Rechenzentrum die vorrangige Gefahr darstellt, sondern schon die davor eintretende Rauchentwicklung. Rauch ist nur wenig wärmer als die Umgebungstemperatur, reine Wärmemelder sprechen darauf nicht an, und schon gar nicht Schmelzloten. Erforderlich ist die Rauchfrüherkennung, et-

wa über Luftansaugung und geeignete Detektion. Die durch den ausgelösten Alarm angesteuerten Brandschutzklappen müssen durch motorischen Antrieb geschlossen werden; bloßes Schließen durch Herunterfallen der Klappen gewährleistet nicht die erforderliche Dichtheit.

Inerte Gase wie CO₂ zum Löschen zu verwenden, bringt die Gefahr des Erstickens allenfalls noch im Raum befindlicher Personen mit sich; für Druckentlastung müssen Vorkehrungen getroffen werden. Alternativen sind, den Sauerstoffgehalt der Luft im Raum auf 15 Prozent zu reduzieren (OxyReduct®) – ein Brand kann sich in dieser Umgebung nicht mehr entwickeln, menschliche Atmung ist jedoch möglich –, oder dem Brand die erforderliche Wärme zu entziehen (Löschmittel Novec 1230®).

Brände außerhalb des Rechnerraums, etwa in einer angrenzenden Garage, können, auch wenn Flammen nicht durchschlagen, durch Strahlungshitze zu einer hohen Erwärmung im Raum führen. Wände, Decken und Fassaden sollten entsprechend gedämmt sein. Die Verglasung von Fenstern und sonstigen lichtdurchlässigen Bauteilen soll nicht nur die Ausbreitung von Feuer und Rauch verhindern (G-Verglasung), sondern auch den Durchtritt der Wärmestrahlung (F-Verglasung).

Zutrittskontrolle. Auch ein ausgeklügeltes Zutrittskontroll- und Schleusensystem nützt nichts, wenn der Rechnerraum über eine Hintertür mit dem Technikerschlüssel betreten werden kann. Nach einer Analyse der Personenströme und ihrer Notwendigkeiten sollen Zugangsberechtigungen zu Sicherheitszonen in einem gestaffelten System reduziert werden. Die Maßnahmen müssen permanent den veränderten Anforderungen angepasst und auch akzeptiert werden, um der Gefahr zu begegnen, dass sie unwirksam gemacht werden.

Einbruchs- und Brandmeldezentrale, Hausleittechnik, Videoüberwachung und Zutrittskontrolle sollen zentral bei einer Stelle zusammenlaufen, von der aus die entsprechenden Reaktionen erfolgen.

Wird mit der Sicherung von Daten ein Dienstleister beauftragt, ergeben sich etliche Rechtsprobleme wie Haftungs-, Lizenz- und Versicherungsfragen. Durch ein Non-Disclosure-Agreement (NDA) ist noch vor Verhandlungsbeginn eine Vereinbarung zur Verschwiegenheit über vertrauliche Informationen, Geschäfts- und Betriebsgeheimnisse zu treffen. Ein Service-Level-Agreement (SLA) soll das Leistungsniveau und die zu fordernde Verfügbarkeit sicherstellen. Zugangsrechte und Aufsichtspflichten sind festzulegen.

„Im IT-Bereich sind häufig Katastrophen anzutreffen, die nicht den klassischen Ausfallszenarien entsprechen“, führte Dipl.-Kfm. Harald Seiffert aus. Fehlerhafte Software führt zu Systemabstürzen, der Rollout eines neuen Programms misslingt, eine Release weist Fehler auf, oder es wird Hardware gestohlen, die für Abläufe von entscheidender Bedeutung ist (Cartridges eines Industrieroboters). Geeignetes Krisenmanagement ist so weit wie möglich vorzuplanen. Bei der Rückstands-aufholung ist zu bedenken, dass immer weniger aufgearbeitet werden kann, je mehr der Betrieb anläuft.

WLAN. Anschlusspunkte (Access Points, AP) für drahtlose Internet-Kommunikation (WLAN) werden immer mehr; sie werden, wenn sie öffentlich auf Bahn- und Flughäfen, in Hotels oder Cafés betrieben werden, für die Datenübermittlung das Gegenstück zur – mittlerweile veralteten – Telefonzelle. Auch Firmen und Private nutzen die Möglichkeiten dieser Technologie. Mobile Computer werden von Kabel-



Sebastian Schreiber: „Entdeckt werden nur die Attacken von Kindern und Vandalen.“

verbindungen unabhängig; man erspart sich das Verlegen von Leitungen.

„Bei War-Driving-Fahrten in Wien und München haben wir durchschnittlich zwei bis drei APs pro Minute ausfindig gemacht“, schilderte Dipl.-Inform. Sebastian Schreiber (www.SySS.de). „48 Prozent der 3.220 überprüften WLANs wurden ohne Verschlüsselung betrieben.“ In derartige Netze kann jedermann, der sich mit seinem WLAN-fähigen Laptop im Funkbereich befindet, eindringen – mit entsprechenden Antennen ist ein Empfang im Kilometerbereich möglich.

Die Standard-Verschlüsselung mit WEP ist durch Schwachpunkte etwa bei der Initialisierung nicht so sicher, wie auf Grund der Schlüssellänge angenommen werden könnte. Zudem erlaubt WEP schwache Passwörter. Mit entsprechenden Tools, die aus dem Internet heruntergeladen werden können, ist es auch Laien möglich, Passwörter zu knacken. Seine Identität als Angreifer zu verschleiern, ist in Minuten-schnelle mit einem Tool möglich, das als Shareware erhältlich ist. „Entdeckt werden nur die Attacken von Kindern und Vandalen“, erläuterte Schreiber.

Es geht bei den Angriffen nicht nur um die Freude am Hacken – auf Kosten des Angegriffenen und unter seiner

Identität können beispielsweise Mehrwertdienste in Anspruch genommen oder urheberrechtlich geschützte Werke (Musik, Filme) raubkopiert werden.

Ist die Vertraulichkeit im WLAN-Betrieb nicht gewährleistet, ist es auch mit der Verfügbarkeit schlecht bestellt. Verbindungen können unterbrochen werden, indem der Angreifer sich bei der Rezeption eines Hotels als Gast ausgibt und sich abmeldet; oder dass dem Gast, angeblich von der Rezeption, mitgeteilt wird, er werde nunmehr abgemeldet; oder dass die Rezeption vor einem Ansturm angeblicher Gäste kapituliert und zusperrt. Eine Rückfrage beim Betroffenen findet in allen diesen Fällen nicht statt; ein Gegenmittel ist bisher noch nicht gefunden worden. Dazu kommen billig herstellbare Störsender, die breitflächig den Funkverkehr stören können.

Abhängigkeit. „Eine alleinige Abhängigkeit von WLAN-Verbindungen sollte vermieden werden“, betont Schreiber. Privat in Firmen aufgebaute Netzwerke, durch die firmeninterne Sicherheitsmaßnahmen unterlaufen werden könnten, können durch Tools wie Netstumbler oder Kismet ausfindig gemacht werden. Beim Kurzstreckenfunk – insbesondere bei mobilen Kleingeräten – hat sich der Standard Bluetooth durchgesetzt. Annehmlichkeiten bei Mobiltelefonen, etwa die Verwendung eines kabellosen Headsets oder einer Freisprecheinrichtung, haben ihren Preis im Verlust von Sicherheit.

Wenngleich auf kürzere Entfernungen als bei WLAN-Nutzung kann man, vom Inhaber unbemerkt, in dessen Mobiltelefon eindringen und gespeicherte Daten (Telefonverzeichnis, SMS) auslesen. „Nicht unbedingt erforderliche Funktionen sollten abgeschaltet werden“, rät Schreiber. „Sie schaffen nur vermeidbare Angriffsmöglichkeiten.“ *Kurt Hickisch*