Special Innovation

Mehr Sicherheit für Server-Räume

Physische Infrastruktur-Security: Die IT eines Unternehmens muss nicht nur vor Hackern geschützt werden.

Sonja Gerstl

IT-Sicherheit ist ein heißes Thema. Dennoch beschränkt sich die Diskussion dabei meist auf virtuelle Bedrohungen wie Viren oder Hacker und die Ausfallsicherheit der Server-Systeme selbst. Was die Verfügbarkeit von IT-Infrastrukturen aber wesentlich massiver bedrohen kann als Software- oder Hardware-Probleme, sind Stromausfälle oder vor externen Einflüssen ungeschützte Server-Räume.

Denn bei einem Stromausfall sind Ausfallzeiten und unter Umständen Datenverlust unvermeidbar. Umso bedeutender für die Ausfallsicherheit von IT-Systemen ist deshalb die Frage nach der baulichen Infrastruktur, die einen unterbrechungsfreien Betrieb gewährleisten kann. Damit neben der IT-Infrastruktur auch die Umwelt geschützt wird, kommen bei Kapsch Business Com auch skalierbare Lösungen zum Einsatz, die mit dem Unternehmen wachsen. Jüngstes österreichisches Referenzprojekt ist der Server-Raum der niederösterreichischen Firma Voith IT Solutions in St. Pölten. Dabei wurde auf etwa 90 Quadratmetern ein Server-Raum der Tier-Klassifikation II+ umgesetzt, die eine jährliche Ausfallzeit von maximal eineinhalb Stunden pro Jahr garantiert.

Ein wesentlicher Aspekt, der bei der Planung eines Server-Raums berücksichtigt werden muss, ist der Standort. „Bei modernen Gebäuden befindet sich der Server-Raum normalerweise nicht im Keller, wo bei Überschwemmungen ein Wassereinbruch drohen könnte, sondern eher in der Mitte des Gebäudes. So werden die Gefahren von außerhalb des Gebäudes möglichst gering gehalten“, erklärt Michael Lamprecht, Leiter des Produktmanagements Infrastruktur bei Kapsch Business Com. Neben Aspekten wie Zutrittskontrolle, Videoüberwachung und Monitoring sowie den besonderen Anforderungen an die Klimatisierung muss die Frage der unterbrechungsfreien Stromversorgung (USV) bereits bei der Planung berücksichtigt werden. „Im Idealfall ist das physische Sicherheitssystem genau an die Anforderungen des Unternehmens angepasst. Wird etwa der Anspruch an die Ausfallsicherheit von 99,99 auf 99,67 Prozent *(28,8 Stunden Downtime pro Jahr, Anm. d. Red.)* gesenkt, fallen die Kosten erheblich“, so Lamprecht.

Die IT von Unternehmen ist einer Reihe von Gefahren ausgesetzt. Um diese zu minimieren, sind zahlreiche Sicherheitsvorkehrungen zu treffen. Foto: Photos.com

Damit auch die Gesamtkosten des Systems möglichst gering gehalten werden, setzt Kapsch vielfach auf modulare Lösungen. Diese Systeme können im laufenden Betrieb erweitert und für die nächste Ausbauphase gerüstet werden.

www.kapsch.net

Kundendaten vor Missbrauch schützen

Internationale Kreditkartengesellschaften erarbeiteten umfangreiches Sicherheitspaket für die Datenverarbeitung.

Online-Einkauf ist noch mehr Vertrauenssache als ein Einkauf in der realen Welt. Das gilt einerseits für die Abwicklung, da ja – im Gegensatz zu Einkäufen in der realen Welt – nicht Zug um Zug abgewickelt werden kann, sprich: Ware gegen Geld. Andererseits gilt das auch für die Kartendaten selbst. In Zeiten von „Hacking“ und „Phishing“ ist die Sensibilität der Konsumenten verständlich. Aber auch im Face-to-Face-Business muss es heißen: Obacht auf die Kartendaten!

Hohe Strafen

Im Fall eines Diebstahls von Kreditkartendaten drohen einem Handelsunternehmen unter anderem neben einem schädlichen Imageverlust auch empfindliche Schadenersatzforderungen durch Kreditkartenorganisationen und Acquirer, sollten diese dem Händler beziehungsweise dessen Service Partner (Payment Service Provider für E-Commerce) nachweisen, dass Sicherheitsanforderungen in der Kreditkartenverarbeitung nicht eingehalten wurden.

Deshalb ist vorgesehen, dass alle, die Kartendaten speichern, technische sowie organisatorische Maßnahmen zum Schutz gegen den Verlust von höchst sensiblen Kartendaten vornehmen. Diese Maßnahmen werden im sogenannten „Payment Card Industry – Data Security Standard“ (PCI DSS) geregelt.

Um das Risiko von Datendiebstählen von vornherein zu minimieren, haben sich die großen internationalen Kreditkartengesellschaften auf diesen Sicherheitsstandard geeinigt, der für die sichere Speicherung und Verarbeitung der Kreditkartendaten sorgen soll. Diesem Standard unterliegen alle Institutionen, wo Daten – auf welche Art und Weise auch immer – verarbeitet und/oder gespeichert werden. PCI Data Security (PCI DSS) stuft Händler in vier verschiedene Levels ein. Je nach Level sind unterschiedliche Schritte seitens des Unternehmens durchzuführen.

Gerade beim Online-Einkauf ist es wichtig, dass sensible Kundendaten auch entsprechend geschützt sind. Foto: Photos.com

Jedes Vertragsunternehmen muss PCI DSS einhalten – Acquirer wie Paylife empfehlen generell, dass keine Kartendaten gespeichert werden, um höchstmögliche Sicherheit zu gewährleisten. Werden Daten gespeichert, muss sich der Händler regelmäßigen Sicherheitsüberprüfungen unterziehen. Wer die vorgegebenen Maßnahmen erfüllt und die vorgeschriebenen Vorkehrungen trifft, wird im Fall der Kompromittierung teilweise beziehungsweise vollständig von Strafen befreit.

Das gilt auch für alle Webshop-Betreiber, die Kartendaten in ihren Systemen speichern. Da das mit Aufwand verbunden ist, geht der Trend eindeutig dahin, dass Webshops Kreditkartendaten nicht mehr selbst speichern, sondern generell die Zahlung über PSP (Payment Service Provider) abwickeln. *sog*

www.paylife.at