Zeitgemäß **gesichert**

von David Ferré

Viele Kommunalverwaltungen und kommunale Rechenzentren beschäftigen sich derzeit mit der Einführung komplexer Konzepte zur umfassenden Absicherung ihrer IT-Netzwerke. Zu Recht: Spät entdeckte Sicherheitslücken können fatale Folgen haben.

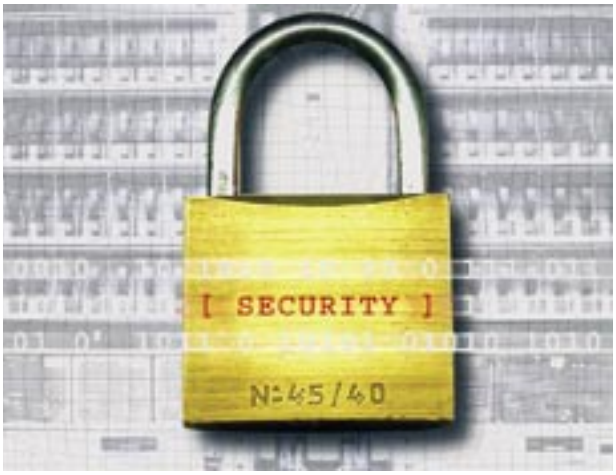
Kommunale Rechenzentren sind sicher. Das stimmt und soll auch so bleiben. Angesichts neuer Trends in der IT wie der zunehmenden Öffnung auch des Zentralrechners für immer mehr Nutzer etwa via Internet kommen neue Aufgaben auf die Sicherheitsverantwortlichen zu. Um das bekannt hohe Sicherheitsniveau wahren zu können, werden vielfach individuelle ganzheitliche Sicherheitskonzepte erarbeitet. Diese beziehen nicht nur die IT-Anwendungen ein, sondern auch die Anwender.

Denn die Vereitelung von Datenübergriffen liegt nicht mehr alleine in der Hand der Verantwortlichen im Rechenzentrum, sondern zunehmend auch bei den Nutzern von IT-Systemen. Diese müssen ein Verständnis für die Notwendigkeit von Sicherheitsmaßnahmen entwickeln und auch verstehen, welche Aspekte in die zentral definierten ganzheitlichen Sicherheitskonzepte hineinspielen.

Kommunale IT-Netzwerke werden zunehmend komplexer. Zahlreiche Anwendungen werden auf verschiedenen IT-Plattformen betrieben und über leistungsfähige Datennetze für eine Vielzahl von Mitarbeitern in dezentralen kommunalen Einrichtungen zugänglich gemacht. Darüber hinaus zählt es zu einem zeitgemäßen Erscheinungsbild einer Kommune, Bürgern Service-Leistungen via Internet anzubieten. Doch mit der Öffnung der IT-Netze für Bürger und Untenehmen läuft man als Verwaltung immer auch Gefahr, Hacker einzuladen.

Die Absicherung von IT-Systemen ist kein neues Thema, im Gegenteil: Der gute Ruf des Zentralrechners in punkto Sicherheit rührt von einem frühen und intensiven Engagement bei seiner Absicherung her. Allgemein gesprochen: IT-Sicherheit wurde früher als punktuelle Absicherung einzelner Anwendungssysteme praktiziert. Die Summe aller Einzelmaßnahmen ergab auf diese Weise die Gesamtheit der IT-Sicherheit. Dieses Prinzip wurde nicht nur auf dem Mainframe, sondern auch in Unix- und PC-Welten in dieser Form fortgeführt.

Derartig abgesicherte Netzwerke können bei zunehmender Komplexität nicht mehr auf wirtschaftliche Weise betrieben werden: Entweder ist der Einsatz von Manpower unvertretbar hoch, oder die Vielfältigkeit der Netzwerke überfordert die dafür verantwortlichen Mitarbeiter. Das führt zu Sicherheitslücken, die früher oder später aufgedeckt werden. Dementsprechend werden heute neue Ansätze praktiziert. Ganzheitliche Sicherheitskonzepte gewinnen zunehmend an Bedeutung. Diese fokussieren eine stringente und durchgängige Sicherheitsinfrastruktur. Derartige Sicherheitskonzepte basieren auf einer zentral definierten Security-Policy, die Regeln, Prüfungsvorschriften und festgelegte



IT-Sicherheit: In Zeiten des Internets ohne Alternative.

Reaktionsverfahren für den Krisenfall beinhaltet. Damit wird ein wesentlicher Unterschied zu der traditionellen Methode deutlich: Ganzheitliche Sicherheitskonzepte beziehen neben allen Anwendungen auch das Verhalten der Mitarbeiter ein.

Bereits auf der organisatorischen Ebene wird bei ganzheitlichen Sicherheitskonzepten die Basis für eine umfassende IT-Sicherheit gelegt. Verantwortlichkeiten für sicherheitskritische Ressourcen und Anwendungen werden definiert, Benutzerrechte und deren Verwaltung zentral geregelt und Regeln zum Gebrauch von Passwörtern festgelegt. Vorschriften, wer für welche Rollen zugelassen wird und damit auf bestimmte Daten und Anwendungen zugreifen darf sind ebenso definiert, wie die Art und Weise, auf die neue Anwender zugelassen werden. Maßnahmen für Schulungen und Verpflichtungen der Mitarbeiter runden auf der organisatorischen Ebene das Konzept ab.

Diese Richtlinien betreffen jeden Bildschirmarbeitsplatz. Doch reicht die Definition von Richtlinien allein nicht aus, um ein hohes Maß an IT-Sicherheit zu gewährleisten. Die für alle Anwender und Anwendungen geltenden zentralen Vorgaben einer durchgängigen und in sich geschlossenen Security-Politik müssen auch in den entsprechenden Anwendungen festgeschrieben werden. Dabei ist eine zentrale Verantwortung in der Sicherheitspolitik Voraussetzung für eine effiziente Administration und damit auch einer einfachen Durchsetzung stringenter Sicherheitsvorschriften. Zudem unterstützen zentrale Strukturen auch eine optimale Kontrolle der Einhaltung von Sicherheitsvorschriften. So müssen beispielweise auch Auditoren bei ihren regelmäßigen Überprüfungen der Einhaltung von Maßgaben der Security-Policy von vornherein in ihrer Arbeit unterstützt werden. Dazu zählt nicht zuletzt die Möglichkeit für Auditoren, zu jeder Zeit und auch ohne Unterstützung speziell ausgebildeter System-Experten komplexe Anwendungsumgebungen zu überprüfen.

Mitarbeiter: Feste Größe beim Security-Management.

Bei der Überprüfung der IT-Sicherheitsinfrastruktur werden häufig systematische Lücken entdeckt – selbst im Bereich des Mainframe-Computing. Ein Beispiel: IBM-Großrechner sind vielfach über das Schutzsystem Resource Access Control Facility (RACF) abgesichert. RACF steht in Fachkreisen als Synonym für IT-Sicherheit. Doch stehen die Meldungen aus RACF häufig den Verantwortlichen erst nach der nächtlichen Produktion, der so genannten Batchbearbeitung, zur Verfügung. Erst nach der manuellen Auswertung kann festgestellt werden, ob und wenn ja, wann und wo ein Sicherheitsverstoß vorgelegen hat. Dieser Zustand ist bei der zunehmenden Öffnung des Mainframes für eine Vielzahl von Nutzern etwa durch Anwendungen im Internet nicht mehr zeitgemäß. Durch die zeitliche Verzögerung und – durch die Vielzahl der in RACF registrierten Meldungen bedingt – die häufig nur stichprobenartige Auswertung dieser Listen können wichtige Sicherheitsmeldungen „untergehen“.

Mit der Einführung komplexer Konzepte zur umfassenden Absicherung von IT-Netzwerken beschäftigen sich daher viele Rechenzentren. Vielfach werden externe Fachberater wie die der Beta Systems Software AG, Berlin, hinzugezogen. Diese bringen das notwendige IT-Fach-Know-how ein, um derartige Konzepte frühzeitig auf die technischen Anforderungen der vorhandenen IT-Infrastruktur abzustimmen. Zum anderen verfügen diese externen Berater aber auch über die fachliche Kompetenz, die es ihnen gestattet, die Notwendigkeiten für ein geschärftes Sicherheitsbewusstsein auch in die Fachabteilungen einer Verwaltung tragen zu können. Denn die Realisierung des ganzheitlichen Sicherheitskonzeptes muss zwar einerseits technisch fundiert sein, andererseits aber auch die fachlichen Prozesse berücksichtigen und sich in die Arbeitsstrukturen einfügen.

David Ferré ist Director Business Unit Data Center Management der Beta Systems Software AG, Berlin.