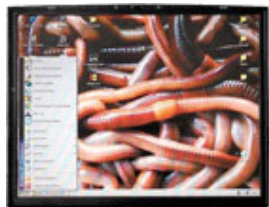


Schäden durch Ausspionierung von Daten

Security wird Thema im Mittelstand

82% der 200 von IDC im Februar und März 2006 zum Thema IT-Sicherheit befragten mittelständischen Unternehmen haben bereits leidvolle Erfahrungen mit Angriffen auf die IT-Infrastruktur machen müssen.



HB FRANKFURT. Die Bedrohungspotenziale sind im wesentlichen die "üblichen Verdächtigen" wie zum Beispiel Viren, Spam, Trojaner und der Datenverlust durch unbeabsichtigtes Löschen. Einige Unternehmen waren aber durchaus auch schon Denial-of-Service-Attacken, Zugangsversuchen zum IT-System durch unberechtigte externe Nutzer oder auch mit Manipulationsversuchen bei Informationen und Systemeinstellungen konfrontiert.

Lediglich 18% der Befragten haben angegeben, dass sie in dieser Hinsicht noch keinerlei Erfahrungen gemacht haben. Die wenigsten dieser Unternehmen mögen sich in der glücklichen Lage befinden, tatsächlich noch keine Probleme mit Angriffen auf die IT-Sicherheit gehabt zu haben. "Auch diese Unternehmen werden irgendwann mit den sich stetig verändernden Bedrohungspotenzialen konfrontiert und sollten für den Tag X entsprechend vorbereitet sein", rät Martin Haas, Consulting Director bei IDC in Frankfurt und Projektleiter der Studie.

Der wesentlich größere Teil dieser vermeintlich unangegriffenen Unternehmen wird allerdings vermutlich eher unbemerkt mit derartigen Problemen konfrontiert worden sein. In diesen Fällen ist zwar die Antwort korrekt, die Konsequenzen sind aber umso dramatischer: "Nichts ist gravierender als ein IT-System, das Bedrohungspotenzialen ausgesetzt ist, die unbemerkt real werden", stellt Haas fest. "Insbesondere der Verlust von Daten oder das Ausspionieren von Kundendaten kann zu umfassenden betriebswirtschaftlichen Schäden führen."

Vor diesem Hintergrund ist der Aufbau einer ganzheitlichen Sicherheitsinfrastruktur dringend zu empfehlen. Eine solche Lösung basiert auf den zuvor definierten Zielen einer Sicherheitslösung, die idealerweise mit den strategischen Unternehmenszielen verknüpft wird. Hieraus ergeben sich die individuellen Sicherheitsanforderungen des Unternehmens, die über eine Kombination aus Hardware- und Software-Produkten sowie Dienstleistungen und Sicherheitsrichtlinien erfüllt werden sollten.

Zahlreiche Unternehmen haben in dieser Hinsicht einen entsprechenden Optimierungsbedarf erkannt und wollen in den nächsten zwei bis drei Jahren das aktuelle Niveau ihrer IT-Sicherheit verbessern.

Offensichtlich ist das nicht nur ein Lippenbekenntnis der Interviewpartner, sondern für diese Aufgabe sollen auch entsprechende finanzielle Mittel bereitgestellt werden", zeigt sich Haas positiv überrascht. Lediglich sieben Prozent der Befragten geben an, dass ihre Ausgaben für die Gewährleistung der IT-Sicherheit in den nächsten zwei bis drei Jahren sinken werden.

Mit der Verbesserung des Sicherheitsniveaus ist auch eine zunehmende Komplexität der Gesamtlösung in den Unternehmen verbunden. "Deshalb ist davon auszugehen, dass zumindest Teile der Sicherheitslösung in Form von Managed Services in Anspruch genommen werden", so Haas. „Die Anbieter von Produkten und Dienstleistungen im Umfeld der IT-Sicherheit dürften in den nächsten Jahren von den lukrativen Marktpotenzialen profitieren.“