Special Innovation

Datenklau lässt sich verhindern

Das Internet ist eine simple Angelegenheit – für Nutzer. Es verleitet aber auch zum leichtfertigen Umgang mit sensiblen Daten in der virtuellen Welt. Das wiederum wissen auch die Hacker und nutzen es schamlos aus.

Die Zahl der Personen, die auch übers Internet kommuniziert, wächst beständig. Die Einfachheit des Systems animiert aber auch zum sorglosen Umgang mit privaten Informationen.

Sonja Gerstl

Cyberkriminelle nutzen zunehmend Sicherheitsschwachstellen in Unternehmen, um auch an die Daten der Kunden dieser Unternehmen zu gelangen. Das ist eines der zentralen Ergebnisse des *IBM X-Force Trend und Risiko Report 2008*, der heuer veröffentlicht wurde. So etwa ist die Zahl der Hacker-Angriffe, die im vergangenen Jahr von seriösen Unternehmenswebsites ausgingen, laut Report alarmierend angestiegen. Fazit: Unternehmen werden zusehends zum Sicherheitsrisiko für ihre eigenen Kunden.

Grobe Security-Lücken

Webseiten, das zeigt der Report sehr deutlich, sind zur Achillesferse der IT-Sicherheit von Unternehmen geworden. Cyberkriminelle konzentrieren ihre Angriffe auf Internet-Anwendungen der Unternehmen, um die PC der Nutzer zu infizieren. Viele Firmen sind nicht richtig davor geschützt: Sie nutzen oft Standard-Lösungen, die mit vielen Schwachstellen behaftet sind. Oder noch schlimmer: Sie arbeiten mit individuellen Lösungen, die Schwachstellen aufweisen, die nicht gepatcht, das heißt korrigiert werden können.

Im vergangenen Jahr hatte mehr als die Hälfte aller offengelegten Schwachstellen in irgendeiner Form mit Web-Anwendungen zu tun – und mehr als 74 Prozent davon hatten keinen Patch. Thomas Hoffmann, Security-Spezialist von IBM ISS Österreich: „Das schwächste Glied in der Kette aus Hard- und Software ist derzeit der Webbrowser. Dazu kommt, dass der Zugang zum Internet so gewöhnlich geworden ist, dass man diesen quasi arglos benutzt. Das wissen auch die Hacker." Vor unliebsamen Konfrontationen mit den Schattenseiten der virtuellen Welt schützt man sich, so Hoffmann, „ vor allem dadurch, dass man nicht der falschen Meinung aufsitzt, dass die Firewall dafür ausreichend ist." Vielmehr seien hier sogenannte Intrusion-Protection-Systeme (IPS) notwendig. Hoffmann: „Während die Firewall so funktioniert wie eine Regelung für Autos, die nach der Farbe Verkehr zulässt oder nicht, schaut ein IPS quasi in den Kofferraum, schützt also auch contentbezogen. Vereinfacht gesagt: Die Firewall kümmert sich bei einem Unfall, dass alles wieder richtiggestellt wird; ein IPS verhindert den Unfall."

Ein Anbieter wie IBM sei, so Hoffmann, bestens ausgerüstet, mit der Vielzahl von Bedrohungen und den sich schnell verändernden Angriffen umzugehen: „ISS untersucht ja seit Jahrzehnten dieses Feld und hat riesiges Know-how gesammelt." Mittelfristig wären optimaler Schutz und Sicherheit im Internet nur gewährleistet, wenn man eine Neudefinition von „Security" in Betracht zieht. Hoffmann: „Gefordert ist eine kooperative Security, die ein Zusammenspiel von Technik und Organisation, also Firmen und Services, gewährleistet."

www.ibm.at

Schutz für Dokumente

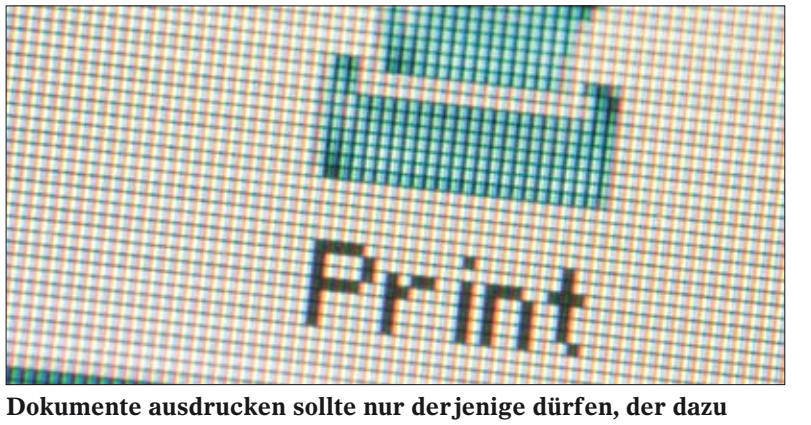
Zugriffskontrolle im Office: innovative Sicherheitslösungen für Drucker und Kopierer.

Sicherheit ist nicht nur für die Informationstechnologie ein Thema. Auch in den Bereichen des Druckens und Kopierens sind entsprechende Maßnahmen notwendig. Die Angebotspalette ist groß und reicht von Druckerzugriffskontrolle über Verschlüsselungslösungen bis hin zur Authentifizierung mittels Fingervenen-Scan – Letztere ist eine Marktinnovation von Konica Minolta.

Sichere Drucker

„Datensicherheit steht heute insbesondere bei Großkunden massiv im Vordergrund: Sie legen großen Wert auf Sicherheitsfeatures. Hochverfügbarkeit ist hier ein passendes Schlagwort. Die Druckerlandschaft muss die Prozesse des Kunden unterstützen, fördern, verbessern und darf diese in keiner Weise behindern. Denn es gibt nichts Unangenehmeres, als aufgrund von Wartungsfehlern keine Ausdrucke zu erhalten oder nicht scannen zu können", beschreibt Johannes Bischof, Geschäftsführer von Konica Minolta Business Solutions Österreich den aktuellen Status quo.

Die Drucker von Konica Minolta verfügen über eine Vielzahl von Sicherheitssystemen, die die Geräte vor unerlaubten Zugriffen schützen. So kann etwa der Raum der IP-Adressen so eingeschränkt werden, dass nur unternehmensinterne Rechner auf den Drucker Zugriff haben. Zusätzlich besteht die Möglichkeit, die Daten sowohl vor dem Transfer zum Drucker als auch auf der Druckerfestplatte zu verschlüsseln und so vor einem Zugriff durch Unbefugte zu schützen. Weiters können gescannte Dokumente automatisch in ein verschlüsseltes PDF-Format umgewandelt werden, sodass sie in weiterer Folge nur von bestimmen Benutzern mittels Passwort geöffnet werden können.



Dokumente ausdrucken sollte nur derjenige dürfen, der dazu auch tatsächlich autorisiert ist. Fotos: Photos.com

Zahlreiche Features wie etwa die Netzwerkauthentifizierung (für den Zugriff auf das System müssen Anwender ein Passwort eingeben), geschütztes Drucken (vor dem Ausdruck geschützter Jobs muss direkt am Bedien-Panel des Systems ein Passwort eingegeben werden) und Datenüberschreibung (Daten werden aus dem Speicher oder von der Festplatte des Systems gelöscht, indem sie mit beliebigen Zeichen überschrieben werden) erhöhen ebenfalls die Sicherheit im Arbeitsalltag. Ganz neu ist die Möglichkeit, heikle Unternehmensdaten via Fingervenen-Scan vor unbefugten Zugriffen zu schützen. Dabei handelt es sich um ein biometrisches Verfahren, das nahezu fälschungssicher ist. Selbst mobiler Content lässt sich auf diese Art noch besser schützen. *sog*

www.konicaminolta.at