



# Bilddateien als neues Schlupfloch für Viren

**PC-Sicherheit** Bisher als sicher geltende JPEG- oder GIF-Dateien können schädlichen Code enthalten

*Virenautoren werden immer raffinierter und flexibler: Nach den Tauschbörsen und Online-Chats entdecken sie Bilddateien als neuen Verbreitungsweg. JPEG- oder GIF-Dateien werden bei der Internetnutzung massenhaft versendet. Bisher wurden solche Dateien meist kategorisch als unproblematisch eingestuft. Jetzt ist es notwendig, sie aufwändig auf Viren zu überprüfen.*

FABIAN HAGLER

Eine kürzlich als Microsoft Image Vulnerability bekannt gewordene Sicherheitslücke hat die Aufmerksamkeit in der IT-Sicherheitsgemeinschaft auf diesen neuen Übertragungsweg gelenkt. Betroffen waren mehrere Programme, unter anderem Windows XP, Office XP und der Service Pack 1 des MS Internet Explorer 6. Bei diesen Anwendungen war es aufgrund eines internen Fehlers möglich, über manipulierte JPEG-Bilddateien auf fremden Rechnern gefährliche Programme auszuführen oder zu installieren. Es genügt also das Öffnen oder Betrachten einer derart manipulierten Datei, um zum Beispiel Dialern, Trojanern oder Keylogging-Programmen den Zutritt zum eigenen Rechner zu gestatten. Auch das Betrachten einer manipulierten Web-Seite reicht aus – sogar die standardmässige E-Mail-Dateivorschau ist gefährlich. Dieser neu entstandene Übertragungsweg hat gravie-

rende Auswirkungen für Unternehmen und ihre Sicherheitsstrukturen: Denn Bilddateien wie JPEGs oder GIFs machen heutzutage einen Grossteil des übertragenen Datenverkehrs aus. Michael Hartmann, Territory Sales Manager DACH & Eastern Europe von Blue Coat, verweist auf intern ausgewertete Daten: «Mit der sprunghaften Verbreitung von schnellen Internetverbindungen für Heimanwender und Unternehmen ist das Web schöner und bunter, aber auch bandbreitenintensiver geworden. Unsere Untersuchungen zeigen, dass mittlerweile fast 30 Prozent des gesamten Internetdatenverkehrs aus Bildern und Grafiken besteht.»

## Internet wird langsamer

Diese 30 Prozent können nicht mehr vom leistungszehrenden Antivirenscan ausgeklammert werden. Damit müssen Unternehmen nun kämpfen: Ihr zu überprüfendes Datenvolumen steigt schlagartig um fast ein Drittel – und die Belastung der Antiviren-Infrastruktur nimmt gravierend zu. Internet heisst für den Nutzer in erster Linie Datenaustausch in Echtzeit. Aber besonders softwarebasierende Virenschutzlösungen operieren, wenn es um die Absicherung von Web-Datenverkehr geht, eng an ihrer Leistungsgrenze. Müssen dabei noch zusätzlich eine Menge Bilder überprüft werden, merkt dies der Nutzer am Desktop – das Internet wird langsamer.

Eine leistungsfähige Web-Antivirenlösung lässt sich deshalb laut der amerikanischen Meta Group nur mit einer Appliance-basierenden Antiviren-Lösung gestalten. Peter Firstbrook, Pro-

gram Director des Beratungsunternehmens, erklärt: «Die neue Virengefahr durch digital übertragene Bilder zwingt viele Unternehmen, ihre bestehenden Sicherheitsregelwerke in Bezug auf Virenschutz zu überdenken. Die üblichen Web-Antivirus-Lösungen bieten hier keinen Leistungsspielraum. Deshalb sollten zukunftsichere Lösungen auf dem Proxy aufsetzen, um auch im Hinblick auf kommende Gefahren die Latenzzeiten bei der Web-Nutzung niedrig zu halten.»

## Tipps für Heimanwender

Für den Privatanwender ist weniger der Performance-Verlust als die Virengefahr durch verseuchte Bilddateien an sich von Bedeutung. Microsoft bewertet die Sicherheitslücke in seinem Security Bulletin als kritisch und empfiehlt die sofortige Installation der bereit gestellten Patches. Weiter gibt Microsoft folgende Tipps: «Lesen Sie E-Mail-Nachrichten im Text-Format, um sich vor Angriffen über HTML-E-Mail-Nachrichten zu schützen.» Dies behebt zwar nicht die zugrundeliegende Sicherheitsschwachstelle, schützt aber vor einer möglichen Angriffsmethode. «Vergewissern Sie sich, dass Ihr Virenschutzprogramm Dateien mit den Endungen JPG bzw. JPEG untersucht.» Viele Virens Scanner beziehen in ihre Suche lediglich besonders gefährdete Dateien (.exe, .com, .vbs etc.) ein. Sollten JPG-Dateien nicht auf der Liste der zu prüfenden Dateien sein, fügen Sie die Endung hinzu oder lassen Sie alle Datei-Typen untersuchen.

**Infos:** [www.microsoft.com/germany/technet/servicedesk/bulletin/ms04-028.msp](http://www.microsoft.com/germany/technet/servicedesk/bulletin/ms04-028.msp)



Medienbeobachtung AG

Mittelland Zeitung Gesamtausgabe

29.09.2004

2 / 3

Auflage/Seite 190098 / 34

1123

Ausgaben 300 /J.

3356029

Blue Coat Systems 25246



**Michael Hartmann** *Der Blue-Coat-Manager warnt vor Viren in Bildern.*

zvg



Medienbeobachtung AG

Mittelland Zeitung Gesamtausgabe

29.09.2004

3 / 3

Auflage/Seite 190098 / 34

1123

Ausgaben 300 /J.

3356029

Blue Coat Systems 25246

Dieser Artikel erschien in folgenden Regionalausgaben:

<i>Titel</i>	<i>Auflage</i>	<i>Titel</i>	<i>Auflage</i>
AZ Aarau	22'426	Limmattaler Tagblatt	11'180
AZ Baden/Zurzach	32'485	Solothurner Zeitung	28'358
AZ Brugg	10'510	Grenchner Tagblatt	5'673
AZ Fricktal	6'540	Berner Rundschau	5'067
AZ Lenzburg	11'061	Langenthaler Tagblatt	5'798
AZ Rheinfelden	4'872	Oltner Tagblatt	19'151
AZ Wohler/Bremgarten	12'050	Zofinger Tagblatt	17'170
AZ Wynental/Zofingen	7'002		