

GFI WHITE PAPER

Gefahren durch tragbare Speichermedien

Wie der unkontrollierte Einsatz von iPods, USB-Sticks und PDAs im Netzwerk zu Datendiebstahl, Virenbefall und rechtlichen Problemen führen kann

Mobile Speichermedien sind überall im Einsatz, ob im privaten oder beruflichen Bereich – doch gerade Unternehmen sind sich oftmals nicht der Sicherheitsgefahr bewusst, die von tragbaren Massenspeichern ausgeht. Dieses White Paper befasst sich mit den Risiken portabler Medien und erläutert, mit welchen Maßnahmen Organisationen der neuen Bedrohung für die Netzwerk- und Datensicherheit entgegenzutreten können.

Einführung

Die digitalisierte Vernetzung unserer Gesellschaft hat auch im Bereich der Datenspeicher zahlreiche technische Innovationen hervorgebracht. Speichermedien werden immer kompakter und mobiler, und der schnelle Zugriff auf MP3-Player, PDAs, Mobiltelefone, Digitalkameras oder USB-Speichersticks bietet Anwendern zahlreiche Vorteile. Trotz dieser Annehmlichkeiten darf jedoch nicht übersehen werden, dass mit dem Aufkommen der neuen Datenträger-Technologie auch zusätzliche Gefahrenquellen für die Sicherheit von Unternehmensnetzwerken entstanden sind. Beispielsweise hat die US-amerikanische Studie „CSI/FBI Computer Crime and Security Survey 2005“ ergeben, dass der Diebstahl proprietärer Daten US-Organisationen im Jahr 2005 Schäden in Höhe von \$355.552 verursacht hat – ein bedeutender Anstieg im Vergleich zum Vorjahr, als der Schaden noch \$168.529 betrug (Gordon et al., 2005).

CSI/FBI Computer Crime and Security Survey 2005

„Die Schäden durch den Diebstahl vertraulicher Daten sind von \$168.529 im Jahr 2004 auf \$355.552 im Jahr 2005 gestiegen.“

Viele Unternehmen, die sich der Bedrohung ihrer Daten durch tragbare Speichermedien bewusst sind, haben bereits Sicherheitsrichtlinien implementiert, die die Verwendung mobiler Datenträger im Unternehmensnetzwerk regulieren sollen. Dennoch bleibt die Frage, ob eine solche Absicherung allein wirksam genug ist. Dieses White Paper geht auf diese Problematik ein und erläutert, welche Risiken bestehen, wenn ein unkontrollierter Zugriff auf tragbare Speichermedien möglich ist.

Einführung.....	2
Wachsende Beliebtheit tragbarer Speichermedien	2
Warum müssen sich Unternehmen vor mobilen Speichermedien schützen?	3
Allgemeine Gegenmaßnahmen	6
Zusammenfassung.....	7
Über GFI Software.....	7
Quellenangaben	7

Wachsende Beliebtheit tragbarer Speichermedien

Die Technologie zur Speicherung elektronischer Daten hat in den letzten zehn Jahren einen bedeutenden Wandel vollzogen. Unhandliche, stationäre Medien mit geringer Speicherkapazität gehören längst der Vergangenheit an. Der technische Fortschritt bei Datenträgern hat folgende Vorteile mit sich gebracht:

- Einen exponentiellen Anstieg bei Speicherkapazität und Datenübertragungsraten
- Eine einfachere Handhabung von Geräten dank immer kompakterer Abmaße

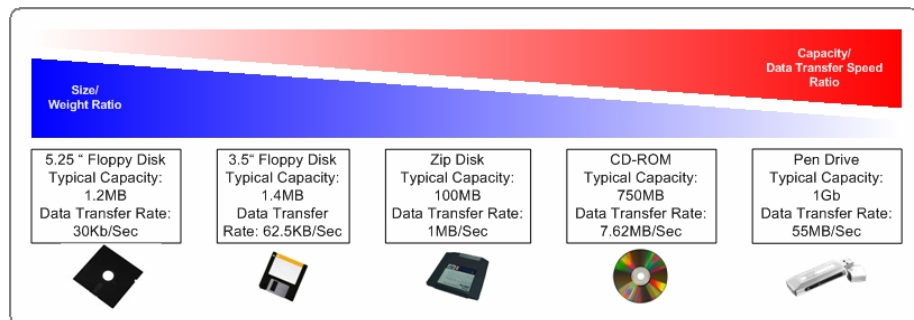
GFI Gefahren durch tragbare Speichermedien

- Eine erfolgreiche Marktdurchsetzung dank für alle Anwenderschichten erschwinglicher Speichermedien
- Vereinfachte Verbindungsmöglichkeiten mit Computersystemen Increased device portability through a substantial reduction in physical device size

Exemplarisch für diese Entwicklung ist der Apple iPod, der im Oktober 2005 auf den Markt kam. Er kann bis zu 60 GB an Daten speichern – dies entspricht der Größe von Festplatten, die üblicherweise in Firmenrechnern ihren Dienst versehen. Mit anderen Worten: Es ist reichlich Speicherplatz für eine immense Anzahl vertraulicher Finanz-, Kunden- und anderer Firmeninformationen vorhanden.

Die Übertragung von Daten zwischen zwei oder mehreren Rechnern kann unauffällig und mit wenigen Mausklicks erfolgen. Solch einfache Handhabung bedeutet ein hohes Sicherheitsrisiko für Unternehmen, da Firmennetzwerke unterschiedlichsten Gefahren ausgesetzt sind.

Beispiele für tragbare Speichermedien



Warum müssen sich Unternehmen vor mobilen Speichermedien schützen?

Laut im Jahr 2005 durchgeführten Analysen des Computer Crime Research Center stehen 98 Prozent aller in Großbritannien gestarteten Angriffe gegen Unternehmen in Verbindung mit internen Mitarbeitern. Datendiebstahl, Schadenersatzansprüche, Produktivitätseinbußen oder eine generelle Kompromittierung der Netzwerkintegrität können die Folge eines unsachgemäßen Gebrauchs mobiler Speichermedien am Arbeitsplatz sein, ob nun durch Insider mit böswilligen Absichten oder auch durch fahrlässig handelnde Mitarbeiter.

Scotland Yard

„98 Prozent aller rechtswidrigen Handlungen gegen britische Unternehmen standen in Verbindung mit internen Mitarbeitern.“

Datendiebstahl

Interne Mitarbeiter können in den meisten Fällen ohne großen Aufwand Unternehmensdaten entwenden. Zudem ist es nicht schwierig, über das Internet an Software zu gelangen, die den Diebstahl sogar automatisiert. Insider müssen nur noch den Datenträger an einen Arbeitsplatzrechner im Unternehmen anschließen, und Informationen jeglicher Art werden unbemerkt und ohne weiteren Benutzereingriff kopiert. Dieser selbsttätige Vorgang ist auch als „Pod-Slurping“ bekannt und erlaubt dank schneller Übertragungsraten selbst das Überspielen ganzer Datenbanken und vertraulicher Inhalte binnen weniger Minuten.

Serious Organized Crime Agency (SOCA) – GB

„... eine der größten Gefahren geht immer noch von vermeintlich vertrauenswürdigen Mitarbeitern aus. Diese unterhöhlen die Sicherheit und starten Angriffe auf das Firmennetzwerk direkt aus dem Unternehmen heraus.“

Datendiebstahl wird jedoch nicht nur von internen Mitarbeiter begangen. Auch Angreifer außerhalb des Unternehmens können sich über das so genannte Social Engineering Informationen erschleichen, indem sie arglose Mitarbeiter dazu verführen, über Unternehmensrechner auf manipulierte Speichermedien, ob in Form von CDs oder USB-Sticks, zuzugreifen. Sind diese Medien mit Malware infiziert, werden Schutzmaßnahmen des Netzwerkperimeters außer Kraft gesetzt und Hintertüren geöffnet, durch die Hacker leichter auf vertrauliche Firmendaten zugreifen können. Wie groß diese Bedrohung ist, zeigen Ergebnisse eines aktuellen Experiments, das von Experten des britischen Schulungsspezialisten The Training Camp durchgeführt wurde (Sturgeon, 2006). Im Rahmen des Versuchs hatten Büroangestellte eine Promotion-CD erhalten. Neben regulären Werbeinformationen enthielt diese auch ein Skript, über das The Training Camp nachverfolgen konnte, wann auf die CD zugegriffen wurde. Obwohl der Datenträger mit dem eindeutigen Warnhinweis versehen war zu überprüfen, ob mit der Verwendung der CD in Unternehmen Sicherheitsrichtlinien verletzt werden könnten, wurden 75 von 100 CDs unkontrolliert im Firmennetzwerk geöffnet. Dieses Experiment verdeutlicht, dass Mitarbeiter, auch wenn sie noch so sehr in gutem Glauben handeln, die Perimetersicherheit kompromittieren können und Unternehmen dadurch ernsthafte Schäden verursachen.

Organisationen arbeiten mit einer Vielzahl unterschiedlicher Daten, die Diebstahl ausgesetzt sein können, z. B.:

- Entwürfe und Konstruktionspläne
- Angebotsunterlagen, Budgetpläne, Kundenlisten, E-Mails und Preislisten
- Kreditkarten- und ähnliche Finanzdaten
- Software-Quellcode und Datenbank-Schemata
- Medizinische Informationen oder andere datenschutzrechtlich relevante Akten
- Verschlusssachen, vertrauliche oder persönliche Daten
- Skripte, Storyboards, Druckunterlagen, Fotos, Videos oder Animationen
- Song-Texte, Tondateien und andere Arten von Audiomaterial

U.S. Secret Service & CERT Coordination Centre

„Aktuelle oder ehemalige Mitarbeiter und Vertragspartner gelten als zweitgrößte Cyber-Bedrohung. Nur Hacker wurden als noch gefährlicher eingestuft.“

GFI Gefahren durch tragbare Speichermedien

Gestohlene Daten können an Wettbewerber verkauft oder von Mitarbeitern, ihren Komplizen oder Hackern auf viele Arten rechtswidrig verwendet werden, z. B. in Form von Identitätsdiebstahl oder für Erpressungsversuche. Auch Mitarbeiter, die zu einem Wettbewerber wechseln, können entwendete Informationen zum Vorteil ihres neuen Arbeitgebers einsetzen oder durch Veröffentlichung vertraulicher Daten das Ansehen ihres früheren Unternehmens schädigen. Umfragen des U.S. Secret Service und des CERT Coordination Center ergaben: „Aktuelle oder ehemalige Mitarbeiter und Vertragspartner gelten als zweitgrößte Cyber-Bedrohung. Nur Hacker wurden als noch gefährlicher eingestuft.“ (Keeney et al., 2005). Diese Angaben werden durch die CSI/FBI-Studie untermauert, bei der 68 Prozent der Teilnehmer angaben, Schäden durch Insider-bedingte Sicherheitsverletzungen erlitten zu haben (Gordon et al., 2006).

2006 CSI/FBI Computer crime and security survey

„68 Prozent der Teilnehmer gaben an, Schäden durch Insider-bedingte Sicherheitsverletzungen erlitten zu haben.“

Gefahr durch Schadenersatzansprüche

Gehen vertrauliche Informationen über tragbare Speichermedien „verloren“, oder werden damit unautorisierte/anstößige Inhalte ins Firmennetzwerk eingeschleust, können Unternehmen unter Umständen dafür haftbar gemacht werden. Je nach Gesetzgebung der unterschiedlichen Länder können durch die Verletzung von Datenschutzrichtlinien Schadenersatzansprüche geltend gemacht werden. Nach dem US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) kann beispielsweise die unerlaubte Veröffentlichung von Gesundheitsdaten, die sich Einzelpatienten zuordnen lassen, mit einer Höchststrafe von \$250.000 und zehn Jahren Gefängnis geahndet werden. In der folgenden Tabelle sind beispielhaft Gesetze und Richtlinien verschiedener Länder aufgeführt.

Land	Gesetze
U.S.A.	Sarbanes Oxley Act, Gramm-Leach-Bliley Act, USA PATRIOT Act, Title 21 of the Federal Regulations Part 11 (21 CFR Part 11), Federal Information Security Management Act, HIPAA
EU	Datenschutz-Direktive, Richtlinien zum Datenschutz und elektronischen Datenverkehr; EU GMP-Leitfaden Annex 11, Computergestützte Systeme
GB	Turnbull Guidance Act [1999], Companies Act, Data Protection Act, Freedom of Information Act, Money Laundering Regulations 2003
Japan	Personal Information Protection Act 2003
Kanada	Personal Information Protection and Electronic Document Act (PIPEDA)
Australien	The Federal Privacy Act (Privacy Act 1988)

Produktivitätseinbußen

Mitarbeiter können Firmenrechner auch für private Zwecke nutzen, indem sie mit Hilfe tragbarer Speichermedien die Perimetersicherheit einfach umgehen und persönliche Dateien direkt im Unternehmen auf den Arbeitsplatzrechner überspielen. Dabei ist unerheblich, ob diese Daten zum Zeitvertreib oder sogar für unternehmensfremde Projekte genutzt werden – wertvolle Arbeitszeit wird verschwendet, und die

GFI Gefahren durch tragbare Speichermedien

Mitarbeiterproduktivität leidet. Dies ist vor allem bei Videospiele der Fall, die zudem gleich mehrere Mitarbeiter von ihren Aufgaben abhalten können.

Verletzung des Netzwerksicherheit

Tragbare Speichermedien am Arbeitsplatz stellen eine Gefahr für die Sicherheit und Funktionsfähigkeit des Unternehmensnetzwerks dar, da sie Viren, Malware oder andere schädlichen Elemente übertragen können – ob vorsätzlich oder unabsichtlich. Sicherheitsbehörden mahnen weiterhin: „ ... eine der größten Gefahren geht immer noch von vermeintlich vertrauenswürdigen Mitarbeitern aus. Diese unterhöhlen die Sicherheit und starten Angriffe auf das Firmennetzwerk direkt aus dem Unternehmen heraus“(Ilett, 2006).

U.S. Federal Trade Commission

„Unzufriedene Mitarbeiter, die Zugang zu Kundenlisten und anderen vertraulichen Informationen erhalten, erweisen sich zunehmend als Gefahr.“

Allgemeine Gegenmaßnahmen

Unternehmen können nur auf eine eingeschränkte Auswahl an Gegenmaßnahmen zurückgreifen, um den unautorisierten Einsatz tragbarer Speichermedien zu verhindern. Viele Organisationen verbieten einfach die Verwendung dieser Medien am Arbeitsplatz und blockieren den Zugang zu entsprechenden Schnittstellen am Rechner. Gruppenrichtlinien unter Windows kommen ebenfalls als Abwehrmethode zum Einsatz. Diese Maßnahmen weisen jedoch einige Nachteile auf:

- Die meisten tragbaren Speichermedien sind sehr kompakt und können daher unbemerkt an den Arbeitsplatz mitgebracht werden.
- Eine differenzierte Unterscheidung zwischen erwünschten und unerwünschten Geräten ist nicht möglich.
- Die Durchsetzung der Abwehrmaßnahmen erfordert einen hohen personellen Aufwand.

Netzwerke lassen sich somit nur mit Hilfe einer spezialisierten Software-Lösung vor den Gefahren unautorisierter mobiler Speichermedien schützen. Diese muss unter Beachtung der unternehmensinternen Sicherheitsrichtlinien zwischen dem erwünschten und unerwünschten Einsatz verschiedener Speichermedien unterscheiden können.

GFI Software unterstützt Organisationen mit einem aktiven Sicherheitsprodukt, das dauerhaft vor Risiken in Form von tragbaren Massenspeichern schützt – GFI EndPointSecurity, die effektive Abwehrlösung gegen firmeninterne Bedrohungen durch mobile Endgeräte. GFI EndPointSecurity ermöglicht die Einschränkung des Datenaustauschs über tragbare Speichermedien und verhindert so den Diebstahl vertraulicher Daten oder die Infizierung von Netzwerken mit Viren und Trojanern. Die Sicherheits-Software unterstützt die aktive Verwaltung des Anwenderzugriffs auf MP3-Player (darunter iPod und Creative Zen), USB-Sticks, CompactFlash- und andere Speicherkarten, PDAs, BlackBerry-Geräte, Mobiltelefone, CDs, Disketten u. v. m. Weitere Informationen und eine Test-Version stehen zum Download bereit unter www.gfisoftware.de/de/endpointsecurity.

Zusammenfassung

Lassen sich tragbare Speichermedien unkontrolliert im Firmennetzwerk verwenden, ist die Unternehmenssicherheit bedeutenden Gefahren ausgesetzt. Böswillige Insider und gutgläubige Mitarbeiter als Opfer von Social Engineering können durch den unautorisierten internen Einsatz mobiler Datenträger mühelos Schutzmaßnahmen überwinden, die nur gegen externe Bedrohungen greifen. Allein darauf zu vertrauen, dass Richtlinien zum Einsatz mobiler Massenspeicher freiwillig und umfassend beachtet werden, reicht nicht aus. Es bleibt somit nur die Implementierung von Sicherheits-Software, mit der sich gezielt und vor allem zentral steuern lässt, welche tragbaren Endgeräte im Firmennetzwerk verwendet werden dürfen. Eine solche Kontrolllösung steht mit GFI EndPointSecurity bereit. GFI EndPointSecurity sorgt dafür, dass lediglich autorisierte Anwender tragbare Speichermedien im Firmennetzwerk nutzen können. Unternehmen werden vor den Gefahren durch mobile Endgeräte abgesichert, und Daten lassen sich effizient und kontrolliert austauschen.

Über GFI Software

GFI Software bietet als führender Software-Hersteller eine umfassende Auswahl an Netzwerksicherheits-, Inhaltssicherheits- und Kommunikationslösungen aus einer Hand, um Administratoren einen reibungslosen Netzwerkbetrieb zu ermöglichen. Mit seiner mehrfach ausgezeichneten Technologie, einer konsequenten Preisstrategie und der Ausrichtung an den Anforderungen kleiner und mittlerer Unternehmen erfüllt GFI höchste Ansprüche an Effizienz und Produktivität. Das Unternehmen wurde 1992 gegründet und ist mit Niederlassungen auf Malta, in London, Raleigh, Hongkong, Adelaide sowie auf Hamburg vertreten und betreut über 200.000 Installationen weltweit. GFI bietet seine Lösungen über ein weltweites Netz von mehr als 10.000 Channel-Partnern an und ist Microsoft Gold Certified Partner. Weitere Informationen stehen zum Abruf bereit unter <http://www.gfisoftware.de>.

Quellenangaben

Kanadisches Parlament (2000) *Personal Information Protection and Electronic Documents Act*, abrufbar unter http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp (zuletzt eingesehen am 28. Juli 2006).

Kommission der Europäischen Gemeinschaften (2000) *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, abrufbar unter http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/com2000-385en.pdf (zuletzt eingesehen am 28. Juli 2006).

Computer Crime Research Center (2005) *Security issues: find the enemy within*, abrufbar unter <http://www.crime-research.org/analytics/security-insider/> (zuletzt eingesehen am 28. Juli 2006).

Europäisches Parlament und Rat der Europäischen Union (2002) *Datenschutzrichtlinie für elektronische Kommunikation*, abrufbar unter <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:DE:HTML> (zuletzt eingesehen am 28. Juli 2006).

Europäisches Parlament und Rat der Europäischen Union (2003) *Annex 11 Computergestützte Systeme, Labcompliance*, abrufbar unter <http://www.labcompliance.com/documents/europe/h-213-eu-gmp-annex11.pdf> (zuletzt eingesehen am 28. Juli 2006).

GFI Gefahren durch tragbare Speichermedien

Federal Trade Commission (1999) *Gramm-Leach Bliley Act*, abrufbar unter <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html> (zuletzt eingesehen am 28. Juli 2006).

Financial Reporting Council (2005) *Internal Control: Guidance for Directors on the Combined Code*, abrufbar unter <http://www.frc.org.uk/documents/pagemanager/frc/Revised%20Turnbull%20Guidance%20October%202005.pdf> (zuletzt eingesehen am 28. Juli 2006).

Gordon L.A., Loeb M.P., Lucyshyn W. und Richardson R. (2005) *2005 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Gordon L.A., Loeb M.P., Lucyshyn W. und Richardson R. (2006) *2006 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Ilett D. (2006) "Trusted insiders" a threat to corporate security, *silicon.com*, abrufbar unter <http://www.silicon.com/research/specialreports/idmanagement/0,3800011361,39158361,00.htm> (zuletzt eingesehen am 28. Juli 2006).

Japanese Government (2003) *Personal Information Protection Act 2003*, abrufbar unter <http://www.privacyexchange.org/japan/PIPA-offtrans.pdf> (zuletzt eingesehen am 28. Juli 2006).

Keeney M., Kowalski E., Cappelli D., Moore A., Shimeall T. und Rogers S. (2005) *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, U.S Secret Service and CERT Coordination Center/SEI.

Leahy P. (2001) *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001*, H.R. 3162 Section-by-section Analysis, abrufbar unter <http://leahy.senate.gov/press/200110/102401a.html> (zuletzt eingesehen am 28. Juli 2006).

NIST Computer Security Division (2002) *Federal Information Security Management Act of 2002*, abrufbar unter <http://csrc.nist.gov/policies/FISMA-final.pdf> (zuletzt eingesehen am 28. Juli 2006).

Office of Legislative Drafting and Publishing (2006) *Privacy Act 1988*, abrufbar unter http://www.privacy.gov.au/publications/privacy88_030706.pdf (zuletzt eingesehen am 28. Juli 2006).

Sarbanes-Oxley (2002) *Sarbanes-Oxley Act of 2002*, abrufbar unter http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley (zuletzt eingesehen am 28. Juli 2006).

Sturgeon W. (2006) *Proof: Employees don't care about security*, *silicon.com*, abrufbar unter <http://software.silicon.com/security/0,39024655,39156503,00.htm> (zuletzt eingesehen am 28. Juli 2006).

United Kingdom Parliament (1989) *Companies Act 1989*, abrufbar unter http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890040_en_1.htm (zuletzt eingesehen am 28. Juli 2006).

United Kingdom Parliament (1998) *Data Protection Act 1998*, abrufbar unter <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm> (zuletzt eingesehen am 28. Juli 2006).

United Kingdom Parliament (2000) *Freedom of Information Act 2000*, abrufbar unter <http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm> (zuletzt eingesehen am 28. Juli 2006).

GFI Gefahren durch tragbare Speichermedien

United Kingdom Parliament (2003) *The Money Laundering Regulations 2003*, abrufbar unter <http://www.opsi.gov.uk/si/si2003/20033075.htm> (zuletzt eingesehen am 28. Juli 2006).

U.S. Food and Drug Administration (2000) *Title 21 Code of Federal Regulations (21 CFR Part 11): Electronic Records; Electronic Signatures*, abrufbar unter http://www.fda.gov/ora/compliance_ref/part11/ (zuletzt eingesehen am 28. Juli 2006).

U.S. Department of Health & Human Services (1996) *Health Insurance Portability and Accountability Act of 1996*, abrufbar unter <http://aspe.hhs.gov/admsimp/pl104191.htm> (zuletzt eingesehen am 28. Juli 2006).



delta technology

Ender Akca
Oberer Ahlenbergweg 7
58313 Herdecke

Telefon: +49 (0)2330 / 80 33 - 0
Telefax: +49 (0)2330 / 80 33 - 29

© 2009 GFI Software. Alle Rechte vorbehalten. Die in diesem Dokument aufgeführten Informationen geben den von GFI Software zum Zeitpunkt der Veröffentlichung vertretenen Standpunkt zum Thema dieses White Papers wieder. Modifizierungen aufgrund von veränderten Marktbedingungen sind vorbehalten. Die in diesem Dokument präsentierten Informationen stellen keine Verpflichtung seitens GFI Software dar, und für ihre Genauigkeit wird nach dem Datum der Veröffentlichung keine Garantie übernommen. Die Angaben in diesem White Paper dienen nur der allgemeinen Information. GFI Software übernimmt keine ausdrückliche oder stillschweigende Haftung für die in diesem Dokument präsentierten Informationen. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANGuard, GFI Network Server Monitor, GFI WebMonitor und die zugehörigen Produktlogos sind eingetragene Marken oder Marken von GFI Software in den Vereinigten Staaten und/oder anderen Ländern. Alle hier aufgeführten Produkte und Firmennamen sind Marken der jeweiligen Eigentümer.