Produkthandbuch

Customer Submission Tool

Version 2.0

McAfee®
Systemschutz

Branchenweit führende Lösungen zum Schutz vor Eindringlingen

McAfee®

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN RECHTSGÜLTIGEN VERTRAG, DER ZU DER VON IHNEN ERWORBENEN LIZENZ GEHÖRT, AUFMERKSAM DURCH. ER ENTHÄLT DIE BESTIMMUNGEN UND DIE BEDINGUNGEN, UNTER DENEN DIE LIZENZIERTE SOFTWARE VERWENDET WERDEN DARF. WENN SIE NICHT WISSEN, WELCHEN LIZENZTYP SIE ERWORBEN HABEN, LESEN SIE IN DEN VERKAUFSUNTERLAGEN, AUFTRAGSUNTERLAGEN ODER LIZENZUNTERLAGEN NACH, DIE DEM SOFTWAREPAKET BEILAGEN ODER DIE IHNEN SEPARAT BEIM KAUF AUSGEHÄNDIGT WURDEN (ALS BROSCHÜRE, ALS DATEI AUF DER PRODUKT-CD ODER ALS DATEI AUF DER WEBSITE, VON DER SIE DAS SOFTWAREPAKET HERUNTERGELADEN HABEN). WENN SIE MIT DEN HIER AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Hinweise

Dieses Produkt enthält oder enthält möglicherweise:

• Software, die im Projekt „OpenSSL“ zur Verwendung im OpenSSL Toolkit entwickelt wurde (hhttp://www.openssl.org/). • Kryptographie-Software, die von Eric A. Young, und Software, die von Tim J. Hudson geschrieben wurde. • Einige Softwareprogramme, für die der Benutzer eine Lizenz (oder Unterlizenz) unter GNU General Public License (GPL) oder anderen ähnlichen freien Softwarelizenzen hält, die es dem Benutzer unter anderem erlauben, bestimmte Programme oder deren Teile zu kopieren, zu ändern und weiter zu verbreiten, und die Zugriff auf den Quellcode gewähren. Bei Software, die GPL unterliegt und in ausführbarem Binärcode an andere Personen weitergegeben wird, muss diesen Benutzern auch der Quellcode zur Verfügung gestellt werden. Der Quellcode der GPL unterliegenden Software ist auf dieser CD einsehbar. Wenn Lizenzen für freie Software erfordern, dass McAfee Rechte zum Nutzen, Kopieren oder Ändern eines Softwareprogramms einräumt, die über die in diesem Vertrag genannten Rechte hinausgehen, dann haben die Rechte bezüglich freier Software Vorrang gegenüber den im Vertrag genannten Rechten. • Ursprünglich von Henry Spencer geschriebene Software. Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Ursprünglich von Robert Nordier geschriebene Software. Copyright © 1996-7 Robert Nordier. • Von Douglas W. Sauder geschriebene Software. • Von Apache Foundation geschriebene Software (http://www.apache.org/). Eine Kopie des Lizenzvertrags für diese Software ist unter www.apache.org/licenses/LICENSE-2.0.txt verfügbar. • Internationale Komponenten für Unicode („ICU“) Copyright ©1995-2002 International Business Machines Corporation und andere. • Von CrystalClear Software, Inc. entwickelte Software, Copyright ©2000 CrystalClear Software, Inc. • FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin. • Outside In® Viewer Technology ©1992-2001 Stellent Chicago, Inc. und/oder Outside In® HTML Export, © 2001 Stellent Chicago, Inc. • Software, die zugunsten von Thai Open Source Software und Clark Cooper urheberrechtlich geschützt ist, © 1998, 1999, 2000. • Software mit Copyright von Expa-Maintainern. • Software, die zugunsten von The Regents of the University of California urheberrechtlich geschützt ist, © 1996, 1989, 1998-2000. • Software, die zugunsten von Gunnar Ritter urheberrechtlich geschützt ist. • Software, die zugunsten von Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., urheberrechtlich geschützt ist, © 2003. • Software, die zugunsten von Gisle Aas urheberrechtlich geschützt ist. © 1995-2003. • Software, die zugunsten von Michael A. Chase urheberrechtlich geschützt ist, © 1999-2000. • Software, die zugunsten von Neil Winton urheberrechtlich geschützt ist, ©1995-1996. • Software, die zugunsten von RSA Data Security, Inc. urheberrechtlich geschützt ist, © 1990-1992. • Software, die zugunsten von Sean M. Burke urheberrechtlich geschützt ist, © 1999, 2000. • Software, die zugunsten von Martijn Koster urheberrechtlich geschützt ist, © 1995. • Software, die zugunsten von Brad Appleton urheberrechtlich geschützt ist, © 1996-1999. • Software, die zugunsten von Michael G. Schwern urheberrechtlich geschützt ist, ©2001. • Software, die zugunsten von Graham Barr urheberrechtlich geschützt ist, © 1998. • Software, die zugunsten von Larry Wall und Clark Cooper urheberrechtlich geschützt ist, © 1998-2000. • Software, die zugunsten von Frodo Looijaard urheberrechtlich geschützt ist, © 1997. • Software, die zugunsten von Python Software Foundation urheberrechtlich geschützt ist, Copyright © 2001, 2002, 2003. Eine Kopie des Lizenzvertrags für diese Software ist unter www.python.org erhältlich. • Software, die zugunsten von Beman Dawes urheberrechtlich geschützt ist, © 1994-1999, 2002. • Von Andrew Lumsdaine, Lie-Quan Lee und Jeremy G. Siek geschriebene Software, © 1997-2000 University of Notre Dame. • Software, die zugunsten von Simone Bordet & Marco Cravero urheberrechtlich geschützt ist, © 2002. • Software, die zugunsten von Stephen Purcell urheberrechtlich geschützt ist, © 2001. • Von Indiana University Extreme! Lab entwickelte Software (http://www.extreme.indiana.edu/). • Software, die zugunsten von International Business Machines Corporation und anderen urheberrechtlich geschützt ist, © 1995-2003. • Von der University of California, Berkeley und deren Autoren entwickelte Software. • Von Ralf S. Engelschall <rse@engelschall.com> für das mod_ssl-Projekt (http:// www.modssl.org/) entwickelte Software. • Software, die zugunsten von Kevlin Henney urheberrechtlich geschützt ist, © 2000-2002. • Software, die zugunsten von Peter Dimov und Multi Media Ltd. urheberrechtlich geschützt ist, © 2001, 2002. • Software, die zugunsten von David Abrahams urheberrechtlich geschützt ist, © 2001, 2002. Die Dokumentation ist unter http://www.boost.org/libs/bind/bind.html verfügbar. • Software, die zugunsten von Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock urheberrechtlich geschützt ist, © 2000. • Software, die zugunsten von Boost.org urheberrechtlich geschützt ist, © 1999-2002. • Software, die zugunsten von Nicolai M. Josuttis urheberrechtlich geschützt ist, © 1999. • Software, die zugunsten von Jeremy Siek urheberrechtlich geschützt ist, © 1999-2001. • Software, die zugunsten von Daryle Walker urheberrechtlich geschützt ist, © 2001. • Software, die zugunsten von Chuck Allison und Jeremy Siek urheberrechtlich geschützt ist, © 2001, 2002. • Software, die zugunsten von Samuel Krempp urheberrechtlich geschützt ist, © 2001. Aktualisierungen, die Dokumentation und eine Historie der Revisionen sind unter http://www.boost.org verfügbar. • Software, die zugunsten von Doug Gregor (gregod@cs.rpi.edu) urheberrechtlich geschützt ist, © 2001, 2002. • Software, die zugunsten von Cadenza New Zealand Ltd. urheberrechtlich geschützt ist, © 2000. • Software, die zugunsten von Jens Maurer urheberrechtlich geschützt ist, ©2000, 2001. • Software, die zugunsten von Jaakko Järvi (jaakko.jarvi@cs.utu.fi) urheberrechtlich geschützt ist, ©1999, 2000. • Software, die zugunsten von Ronald Garcia urheberrechtlich geschützt ist, © 2002. • Software, die zugunsten von David Abrahams, Jeremy Siek und Daryle Walker urheberrechtlich geschützt ist, ©1999-2001. • Software, die zugunsten von Stephen Cleary (shammah@voyager.net) urheberrechtlich geschützt ist, ©2000. • Software, die zugunsten von Housemarque Oy <http://www.housemarque.com> urheberrechtlich geschützt ist, © 2001. • Software, die zugunsten von Paul Moore urheberrechtlich geschützt ist, © 1999. • Software, die zugunsten von Dr. John Maddock urheberrechtlich geschützt ist, © 1998-2002. • Software, die zugunsten von Greg Colvin und Beman Dawes urheberrechtlich geschützt ist, © 1998, 1999. • Software, die zugunsten von Peter Dimov urheberrechtlich geschützt ist, © 2001, 2002. • Software, die zugunsten von Jeremy Siek und John R. Bandela urheberrechtlich geschützt ist, © 2001. • Software, die zugunsten von Joerg Walter und Mathias Koch urheberrechtlich geschützt ist, © 2000-2002. • Software, die zugunsten der Carnegie Mellon University urheberrechtlich geschützt ist, © 1989, 1991, 1992. • Software, die zugunsten von Cambridge Broadband Ltd. urheberrechtlich geschützt ist, © 2001-2003. • Software, die zugunsten von Sparta, Inc. urheberrechtlich geschützt ist, © 2003-2004. • Software, die zugunsten von Cisco, Inc. und Information Network Center of Beijing University of Posts and Telecommunications urheberrechtlich geschützt ist, © 2004. • Software, die zugunsten von Simon Josefsson urheberrechtlich geschützt ist, © 2003. • Software, die zugunsten von Thomas Jacob urheberrechtlich geschützt ist, © 2003-2004. • Software, die zugunsten von Advanced Software Engineering Limited urheberrechtlich geschützt ist, © 2004. • Software, die zugunsten von Todd C. Miller urheberrechtlich geschützt ist, © 1998. • Software, die zugunsten von The Regents of the University of California urheberrechtlich geschützt ist, © 1990, 1993, mit Code aus Software, die von Chris Torek an Berkeley gegeben wurde.

Inhalt

1 Einführung 4

Produktfunktionen 4
Was ist neu in dieser Version? 5
Verbesserter Zugriff auf das Tool 5
Zusätzliche Ziele, an die E-Mails gesendet werden können 6
Automatische Verwendung von Schwarzen und Weißen Listen 6
Keine Beschränkung der Anzahl der Einsendungen 7
Automatisches Löschen nach Einsendung 7
Verwendung dieses Handbuchs 7
Zielgruppe 7
Konventionen 8
Produktinformationen 9
Kontaktinformationen 9

2 Über Spam und Phish 11

Einige nützliche Begriffe 11
Was ist Spam? 12
Spam vermeiden 12
Was ist Phish? 13
Phish vermeiden 13
Was ist das Customer Submission Tool? 14
Bayes'sches Lernen 15
So funktioniert der Spam-Wert 15

3 Installation des Tool 16

Installations-Checkliste 17
Herunterladen der Installationsdateien 18
Manuelle Installation des Tool 18
Installation des Tool mit einem Skript 19
Beispiele 21
Einführung des Tool für E-Mail-Benutzer 22
Ändern der Konfigurierung 23

4 Verwendung des Tool 24

Einsenden Ihres ersten Spam- oder Phishing-Musters 24
Einsenden weiterer Spam- oder Phishing-Muster 25
Einsenden Ihres ersten falsch kategorisierten Musters 26
Einsenden weiterer falsch kategorisierter Muster 27
Hinzufügen Ihrer Microsoft Outlook-Kontakte zur Weißen Liste 27
Konfigurierung des Tool 28

1 Einführung

Das McAfee Customer Submission Tool arbeitet mit der E-Mail-Software Microsoft® Outlook® zusammen, um die Menge unerwünschter E-Mails (oder *Spam*), die Sie erhalten, zu reduzieren. Das Tool leitet E-Mails direkt an McAfee Labs oder andere McAfee-Produkte weiter; dort kann das Muster analysiert und zur Verringerung von weiterem Spam verwendet werden.

Diese Themen werden in diesem Abschnitt behandelt:

- *Produktfunktionen*
- *Was ist neu in dieser Version?* auf Seite 5
- *Verwendung dieses Handbuchs* auf Seite 7

Produktfunktionen

Das McAfee Customer Submission Tool kann verwendet werden mit:

- Secure Content Management-Anwendungen
- McAfee Quarantäne-Manager-Software

Das Tool fügt dem Microsoft Outlook Client Schaltflächen und Menüeinträge hinzu. Dadurch stehen Ihnen die folgenden Optionen zur Verfügung:

- Einsenden von Mustern an McAfee Labs zur weiteren Analyse.
- Einsenden von Mustern an einen McAfee Quarantäne-Manager oder an eine Secure Content Management-Anwendung, um weiteren Spam zu vermeiden.
- Einsenden unerwünschter E-Mails, die nicht als Spam (oder Phish) kategorisiert wurden.
- Einsenden von E-Mails, die fälschlicherweise als Spam (oder Phish) kategorisiert wurden.
- Optional dazu kann die Nachricht nach dem Einsenden gelöscht werden.
- Hinzufügen der E-Mail-Adresse des Absenders einer Spam-Mail zu einer Schwarzen Liste, um weiteren Spam zu vermeiden.

- Hinzufügen der E-Mail-Adresse des Absenders einer E-Mail zu einer Weißen Liste, um zu verhindern, dass weitere E-Mails dieses Absenders fälschlicherweise als Spam oder Phish kategorisiert werden.
- Hinzufügen aller E-Mail-Adressen in Ihren Microsoft Outlook-Kontakten zu einer Weißen Liste, um zu verhindern, dass E-Mails bekannter Kontakte fälschlicherweise als Spam oder Phish kategorisiert werden.

Sie können das Tool mithilfe eines Assistenten installieren. Wenn Sie das Produkt für mehrere E-Mail-Benutzer installieren, können Sie die Installation mithilfe eines Skripts durchführen.

Was ist neu in dieser Version?

Diese Version des Customer Submission Tool beinhaltet die folgenden neuen Funktionen oder Verbesserungen:

- *Verbesserter Zugriff auf das Tool*
- *Zusätzliche Ziele, an die E-Mails gesendet werden können*
- *Automatische Verwendung von Schwarzen und Weißen Listen*
- *Keine Beschränkung der Anzahl der Einsendungen*
- *Automatisches Löschen nach Einsendung*

Verbesserter Zugriff auf das Tool

Frühere Version	Wenn die Betreffzeilen angezeigt werden, sind Schaltflächen in der Standard-Symbolleiste und Einträge im Menü **Aktionen** verfügbar.
Aktuelle Version	Zusätzlich dazu sind Schaltflächen in der Standard-Symbolleiste und Einträge im Menü **Aktionen** verfügbar, wenn eine E-Mail angezeigt wird.
Vorteile	Das Tool ist in Microsoft Outlook in zusätzlichen Situationen verfügbar.
Für weitere Informationen	Siehe *Verwendung des Tool* auf Seite 24.

Zusätzliche Ziele, an die E-Mails gesendet werden können

Frühere Version	Sie können E-Mails an McAfee Labs zur Analyse senden. McAfee kann falsch kategorisierte E-Mails analysieren, um die Entdeckungsrate seiner Anti-Spam-Produkte zu verbessern.
Aktuelle Version	Sie können E-Mails an zusätzliche Anwendungen senden: ■ Eine McAfee-Secure Content Management-Anwendung ■ McAfee Quarantäne-Manager-Software
Vorteile	Die Muster können die Leistung der Bayes'schen Datenbanken verbessern, die lernen können, Spam und Phish und zulässige Nachrichten zu erkennen.
Wo finde ich diese Funktion?	Diese Funktion ist verfügbar, wenn das Tool installiert wird. Sie können es auch später konfigurieren.
Für weitere Informationen	Siehe *Verwendung des Tool* auf Seite 24.

Automatische Verwendung von Schwarzen und Weißen Listen

Frühere Version	Diese Funktion war nicht verfügbar.
Aktuelle Version	Diese Funktion ist verfügbar, wenn Sie das Tool mit dem McAfee Quarantäne-Manager (MQM) verwenden. Absender können automatisch einer Weißen Liste (einer Liste mit vertrauenswürdigen E-Mail-Adressen) oder einer Schwarzen Liste (einer Liste mit E-Mail-Adressen, die bekanntermaßen Spam senden) hinzugefügt werden. Ihre Microsoft Outlook-Kontakte können mit einem einzigen Klick der Weißen Liste hinzugefügt werden.
Vorteile	E-Mails, die von bekannten Spammern gesendet werden, werden in Zukunft automatisch als Spam kategorisiert. E-Mails von vertrauenswürdigen Quellen werden nicht als Spam kategorisiert.
Wo finde ich diese Funktion?	Diese Funktion wird aktiviert, wenn eine E-Mail zur Analyse an MQM gesendet wird.
Für weitere Informationen	Siehe *Hinzufügen Ihrer Microsoft Outlook-Kontakte zur Weißen Liste* auf Seite 27.

Keine Beschränkung der Anzahl der Einsendungen

Frühere Version	Bisher konnten Sie bis zu 10 Muster gleichzeitig einsenden.
Aktuelle Version	Diese Beschränkung trifft nicht mehr zu.
Vorteile	Einsendungen können schneller und einfacher durchgeführt werden.

Automatisches Löschen nach Einsendung

Frühere Version	Sie müssen Spam-Mails (oder Phish-Mails) manuell löschen, nachdem Sie ein Muster eingesendet haben.
Aktuelle Version	Sie können auswählen, dass jede ausgewählte Nachricht sofort gelöscht wird, nachdem sie eingesendet wurde.
Vorteile	Einsendungen können schneller und einfacher durchgeführt werden.

Verwendung dieses Handbuchs

In diesem Handbuch finden Sie Informationen darüber, wie Sie Ihr Produkt konfigurieren und verwenden können. Folgende Themen sind enthalten:

- *Einführung*
  Eine Übersicht des Produkts, einschließlich einer Beschreibung neuer oder geänderter Funktionen, eine Übersicht dieses Handbuchs und McAfee-Kontaktinformationen.
- *Über Spam und Phish*
  Informationen über Spam und Phish und wie sie reduziert werden können.
- *Installation des Tool*
  Herunterladen der Dateien. Verwenden eines Microsoft Windows-Installationsprogramms. Installation mithilfe eines Skripts.
- *Verwendung des Tool*
  Wie Sie Muster senden und das Tool konfigurieren können.

Zielgruppe

Diese Informationen richten sich primär an zwei Zielgruppen:

- Netzwerk-Administratoren, die verantwortlich für die E-Mail-Sicherheit ihres Unternehmens sind.
- Benutzer, die verantwortlich für die Konfigurierung der Entdeckungsoptionen ihrer Software sind.

Konventionen

In diesem Handbuch werden die folgenden Konventionen verwendet:

Schmalfett	Alle Wörter der Benutzeroberfläche, einschließlich Optionen, Menüs, Schaltflächen und Namen von Dialogfeldern. **Beispiel:** Geben Sie den **Benutzernamen** und das **Kennwort** des betreffenden Kontos ein.

`Courier`	Der Pfad eines Ordners oder Programms; Text, der genau wiedergibt, was der Benutzer eingibt (z. B. ein Befehl in der Befehlszeile).
	Beispiele:
	Der Standardort für das Programm lautet:
	`C:\Program Files\McAfee\EPO\3.5.0`
	Geben Sie diesen Befehl auf dem Client-Computer ein:
	`scan --help`

Kursiv	Zur Betonung oder wenn ein neuer Begriff vorgestellt wird; für Namen von Produktdokumentationen und Themen (Überschriften) innerhalb des Materials. **Beispiel:** Weitere Informationen finden Sie im *VirusScan Enterprise Produkthandbuch*.
Blau	Eine Internetadresse (URL) und/oder ein aktiver Link. **Beispiel:** Besuchen Sie die McAfee-Website unter: `http://www.mcafee.com`
<BEGRIFF>	Spitze Klammern umschließen einen allgemeinen Begriff. **Beispiel:** Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf <SERVER>.
	**Hinweis:** Zusätzliche Informationen, z. B. eine zusätzliche Methode, denselben Befehl auszuführen.
	**Tipp:** Vorschläge für optimale Verfahren und Empfehlungen von McAfee in Bezug auf Leistung, Effektivität und die Vermeidung von Bedrohungen.
	**Vorsicht:** Wichtige Hinweise zum Schutz Ihres Computersystems, Ihres Unternehmens, Ihrer Softwareinstallation oder Ihrer Daten.
	**Warnung:** Wichtige Hinweise zum Schutz eines Benutzers vor körperlichen Schäden bei der Verwendung eines Hardware-Produkts.

Produktinformationen

Wenn nicht anderweitig angegeben, erhalten Sie Produktinformationen als Adobe Acrobat-.PDF-Dateien auf der McAfee Download-Website.

Produkthandbuch – Einführung in das Produkt und seine Funktionen; detaillierte Anweisungen für die Installation und Konfiguration der Software; Informationen über die Ausbringung, wiederkehrende Aufgaben und Vorgehensweisen.

Versionshinweise – *ReadMe.* Produktinformationen, behobene Fehler, etwaige bekannte Probleme, in letzter Minute an diesem Handbuch oder seiner Dokumentation vorgenommene Ergänzungen und Änderungen. Eine Textdatei liegt der Software-Anwendung bei.

Lizenzvereinbarung – Die McAfee-Broschüre mit dem Lizenzvertrag, die sämtliche Lizenzarten enthält, die Sie für Ihr Produkt erwerben können. Die Lizenzvereinbarung enthält die allgemeinen Geschäftsbedingungen für die Verwendung des lizenzierten Produkts.

Kontakt – Kontaktinformationen für McAfee-Services und -Ressourcen: technischer Support, Kundendienst, Security Headquarters (AVERT), Beta-Programm und Ausbildung. Eine Textdatei liegt der Software-Anwendung bei.

Kontaktinformationen

Security Headquarters: AVERT

Homepage
http://www.mcafeesecurity.com/us/security/home.asp

Virendatenbank
http://vil.mcafeesecurity.com

AVERT WebImmune, Muster einsenden *(Anmeldedaten erforderlich)*
https://www.webimmune.net/default.asp

AVERT DAT Benachrichtigungsdienst
http://vil.mcafeesecurity.com/vil/join-DAT-list.asp

Download-Website

Homepage
http://www.mcafeesecurity.com/us/downloads/

Anti-Virus DAT-Datei und -Modul-Aktualisierungen
http://www.mcafeesecurity.com/us/downloads/updates/default.asp
ftp://ftp.mcafee.com/pub/antivirus/datfiles/4.x

Anti-Spam-Regeldatei und -Modul-Aktualisierungen
ftp://ftp.mcafee.com/spamdefs/1.x/

Produkt-Aktualisierungen *(Anmeldedaten erforderlich)*
https://secure.nai.com/us/forms/downloads/upgrades/login.asp

Veröffentlichungen von HotFix- und Patch-Dateien für Security Vulnerabilities *(frei erhältlich)*
http://www.mcafeesecurity.com/us/downloads/updates/hotfixes.asp

Veröffentlichungen von HotFix- und Patch-Dateien für Produkte *(ServicePortal-Konto und McAfee-Genehmigungsnummer des technischen Kundendienstes erforderlich)*
https://mysupport.nai.com/products/products.asp

Unterstützung für das Ende der Lebensdauer eines Produkts
http://www.mcafeesecurity.com/us/products/mcafee/end_of_life.htm

Technischer Kundendienst für Software und Hardware

Homepage
http://www.mcafeesecurity.com/us/support/technical_support

KnowledgeBase durchsuchen
http://knowledgemap.nai.com/

McAfee Technischer Kundendienst ServicePortal *(Anmeldedaten erforderlich)*
https://mysupport.mcafeesecurity.com

McAfee Security Alerting Service (MSAS)
http://mysupport.nai.com/supportinfo/psvans_info.asp

Kundendienst

E-Mail
https://secure.nai.com/us/forms/support/request_form.asp

Website
http://www.mcafeesecurity.com/us/support/default.asp

Telefon – USA, Kanada und Lateinamerika gebührenfrei:
+1-888-VIRUS NO oder **+1-888-847-8766** Montag - Freitag, 8 bis 20 Uhr, Standardzeit

Informationen darüber, wie Sie eine McAfee-Niederlassung in Ihrer Nähe kontaktieren können, finden Sie unter:
http://www.mcafeesecurity.com/us/contact/home.htm

McAfee Beta-Programm

http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm

Ausbildung: McAfee University

http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm

2 Über Spam und Phish

Wie das Tool dabei hilft, sie zu reduzieren

In diesem Abschnitt werden die Funktionen des Tool beschrieben und wie es mit anderen McAfee-Sicherheitsprodukten zusammenarbeitet, um Spam zu reduzieren.

- *Einige nützliche Begriffe*
- *Was ist Spam?* auf Seite 12
- *Spam vermeiden* auf Seite 12
- *Was ist Phish?* auf Seite 13
- *Phish vermeiden* auf Seite 13
- *Was ist das Customer Submission Tool?* auf Seite 14
- *Bayes'sches Lernen* auf Seite 15
- *So funktioniert der Spam-Wert* auf Seite 15

Einige nützliche Begriffe

Die folgenden Definitionen sind möglicherweise nützlich für Sie:

- **falsch negativ** – Eine E-Mail, die nicht kategorisiert wurde, aber Inhalt enthält, der generell als Spam oder Phish betrachtet wird.
- **falsch positiv** – Eine E-Mail, die als Spam oder Phish kategorisiert wurde, die der Empfänger aber nicht als Spam oder Phish betrachtet.
- **Spammer** – Eine Person oder Organisation, die Spam erzeugt.
- **Spoofing** – Beispiele wären das Fälschen der Herkunft einer E-Mail, um die Identität des Absenders zu verbergen, oder das Erstellen einer Website, die authentisch wirkt.
- **Weiße Liste** – Eine Liste genehmigter Absender.
- **Schwarze Liste** – Eine Liste der Absender, die Spam oder Phish senden.

Was ist Spam?

Alle unerwünschten und unwillkommenen E-Mails können als Spam betrachtet werden. Spam (auch bekannt als Unsolicited Bulk Email (UBE), also unverlangter, massenhafter Versand von Nachrichten) beinhaltet kommerzielle E-Mails, die das elektronische Gegenstück zu *Reklamesendungen* darstellen, und unverlangte nichtkommerzielle E-Mails wie beispielsweise fingierte Virenwarnungen, Witze und Kettenbriefe.

Oft fälschen die Personen, die Spam erstellen und als *Spammer* bekannt sind, die Kopfzeilen der E-Mails, um ihre wahre Identität zu verbergen, wodurch vergeltende Maßnahmen oft auf Unschuldige umgelenkt werden.

Was ist nicht-Spam?

Es gibt E-Mails, die als Spam bezeichnet werden, aber kein Spam sind. Wenn Sie beispielsweise einen Newsletter oder ein Online-Forum abonniert haben oder Informationen über ein Produkt angefordert oder vor kurzem eine Workgroup verlassen haben, befindet sich Ihre E-Mail-Adresse wahrscheinlich noch auf einer Verteilerliste. Um diese Art ungewünschter E-Mails zu reduzieren, entfernen Sie Ihre E-Mail-Adresse sofort aus allen Verteilerlisten, die nicht mehr aktuell sind.

Spam vermeiden

Jedes Mal, wenn Sie eine E-Mail-Adresse verwenden, um Nachrichten zu senden oder auf sie zu antworten, um in einem Internet-Chatroom zu posten oder eine E-Mail-Adresse bekannt zu machen, setzen Sie dieses E-Mail-Konto *Spammern* aus. Spammer stellen Listen von E-Mail-Adressen zusammen. Mit der Zeit wird die Adresse zu immer mehr Listen innerhalb der Spammer-Netzwerke hinzugefügt, wodurch die Menge an Spam, die Sie erhalten, immer größer wird.

Befolgen Sie alle Richtlinien über die Verwendung von E-Mails, die Ihre Organisation zur Förderung von richtigem Umgang mit E-Mails empfiehlt. Dadurch können Sie die Anzahl der Spam-Mails, die Sie erhalten, reduzieren. Zum Beispiel:

- **Hüten Sie sich davor, Produkte zu kaufen, für die mit Spam-Mails Werbung gemacht wird.** Dadurch wird der Spammer darauf aufmerksam, dass die E-Mail-Adresse aktiv ist, diese Adresse kann dann an weitere Spammer verkauft werden. Außerdem geben Sie persönliche Informationen preis.
- **Veröffentlichen Sie keine persönliche Adresse online.** Verwenden Sie stattdessen eine *Wegwerf*-Adresse, wenn Sie an Newsgroups oder Wettbewerben teilnehmen oder wenn jemand Ihre E-Mail-Adresse wissen will. Wenn diese Adresse übermäßig viel Spam empfängt, können Sie aufhören, diese Adresse zu verwenden, und eine neue Adresse erstellen.
- **Antworten Sie nicht auf Spam-Mails**, **auch wenn diese anbieten, Sie von der Verteilerliste zu streichen.** Durch Ihre Antwort wird der Spammer darauf aufmerksam, dass die E-Mail-Adresse aktiv ist; diese Adresse kann dann an weitere Spammer verkauft werden.

Unter *So funktioniert der Spam-Wert* auf Seite 15 finden Sie Informationen darüber, wie Sie mit einer sorgfältigen Konfiguration von McAfee-Anti-Spam-Produkten Spam reduzieren können.

Was ist Phish?

Einige Spammer spezialisieren sich darauf, E-Mails zu *spoofen*, um ahnungslose E-Mail-Benutzer dazu zu bringen, Informationen über ihre Identität und Geldkonten preiszugeben. Diese spezialisierte Form von Spam ist bekannt als *Phish*.

In der Regel empfangen Sie E-Mails, die scheinbar von einer vertrauenswürdigen Organisation wie z. B. einer Bank zu kommen scheinen. Die E-Mail leitet Sie normalerweise an eine *gespoofte* Website weiter, auf der Sie nach persönlichen und finanziellen Details wie z. B. Kontonummern, Kennwort, Kreditkartendetails und Sozialversicherungsnummer gefragt werden. Kriminelle können die gestohlene Identität verwenden, um auf betrügerische Weise Waren und Dienstleistungen (wie z. B. persönliche Kredite) zu erwerben, um direkt von Ihrem Konto zu stehlen oder um Bankkonten zu eröffnen und Geld zu waschen.

Phish vermeiden

- **Vorsicht vor allen E-Mails, die nach Kennwörtern oder anderen sensiblen Informationen fragen.** Banken fragen nicht direkt nach solchen Informationen und verifizieren in der Regel Informationen, indem sie die Post verwenden. Es ist unwahrscheinlich, dass eine Organisation Ihre Kontoinformationen *verloren* hat. Die übliche Prozedur wäre, Ihnen neue Details per Post zukommen zu lassen, anstatt Sie zu bitten, die Details per E-Mail oder über eine Website preiszugeben,
- **Vorsicht vor Links auf Websites.** Wenn Sie gebeten werden, sensible Informationen anzugeben, werden Sie möglicherweise über einen *gespooften* Link weitergeleitet. Ein Beispiel wäre ein Link in einer E-Mail, der nach der Website Ihrer Bank aussieht (www.beispiel.de) und Sie mit einer Website verbindet, die authentisch aussieht. Allerdings zeigt die Adresse im Browser stattdessen einen anderen Namen (z. B. www.beispiel.net) oder eine IP-Adresse (z. B. 168.192.255.200) an.
- **Vorsicht vor unsicheren Websites.** Seriöse Organisationen betreiben sichere Websites, die Ihre persönlichen Informationen verschlüsseln, bevor Sie sie senden. Die Websites solcher Organisationen haben Adressen wie z. B. https://www.beispiel.de statt http://beispiel.de. In anderen Worten, sie verwenden ein gesichertes Internet-Protokoll namens **https** statt **http**.

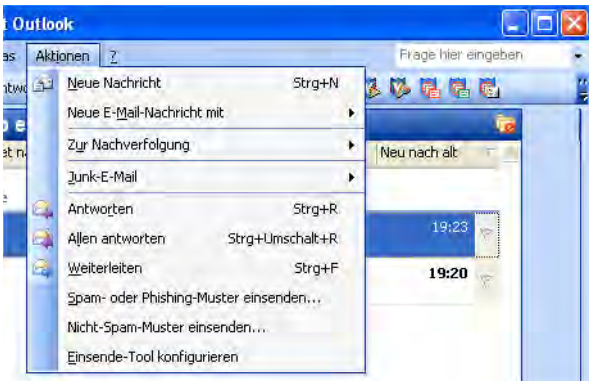
Was ist das Customer Submission Tool?

Anti-Spam-Produkte bieten guten Schutz gegen Spam. Allerdings ist Spam mitunter schwer zu entdecken; Spammer entwickeln neue Techniken, und mancher aktuelle Spam wird zwangsläufig von *keinem* Anti-Spam-Produkt entdeckt. Zusätzlich können falsche Erkennungen auftreten, wodurch ein Anti-Spam-Produkt fälschlicherweise authentische E-Mails als Spam kategorisiert.

Durch die Analyse von neuem Spam (und Phish) und falsch kategorisierten E-Mails können die Anti-Spam-Produkte von McAfee kontinuierlich verbessert werden.

Das Customer Submission Tool arbeitet mit der E-Mail-Software Microsoft Outlook zusammen, um die Menge unerwünschter E-Mails (oder *Spam*), die Sie erhalten, zu reduzieren. Zusätzliche Schaltflächen und Menüeinträge werden verfügbar, wenn Sie Ihre E-Mail lesen.

Abbildung 2-1 Zusätzliche Schaltflächen und Menüs in Microsoft Outlook



Das Tool kann E-Mails an McAfee Labs oder an andere McAfee Anti-Spam-Produkte zur Analyse weiterleiten:

- **Senden einer E-Mail an McAfee Labs**
  Wir arbeiten daran, die Erkennung in unseren Anti-Spam-Produkten konstant zu verbessern. Wir untersuchen E-Mails, die fälschlicherweise durch unsere Software oder die Produkte anderer Hersteller kategorisiert wurden, lernen, *warum* dies der Fall war, und verbessern dadurch unsere Anti-Spam-Produkte.

  Wir behandeln alle eingereichten Muster als vertrauliches Material; wir leiten sie weder weiter, noch verwenden wir sie zu einem anderen Zweck als zu Forschung. Um das Muster richtig zu analysieren, untersuchen wir die Kopfzeile der E-Mail, einschließlich Absender und Betreff, und den Inhalt der Nachricht, einschließlich Text und Anhängen. Unsere gesamte Datenschutzrichtlinie wird angezeigt, wenn Sie das Tool installieren.

- **Senden einer E-Mail an eine Secure Content Management (SCM)-Anwendung**
  Wenn das Netzwerk durch eine SCM-Anwendung geschützt ist, können Sie Muster an eine Anwendung für Bayes'sches Lernen senden. Siehe Seite 15.

- **Senden einer E-Mail an den McAfee Quarantäne-Manager (MQM)**
  Wenn das Netzwerk MQM-Software beinhaltet, können Sie Muster an den McAfee Quarantäne-Manager für Bayes'sches Lernen senden. Siehe Seite 15.

Bayes'sches Lernen

Die Secure Content Management (SCM)-Anwendungen und der McAfee Quarantäne-Manager (MQM) verwenden eine Datenbank, die auf dem Bayes-Theorem der Wahrscheinlichkeit basiert, um zu bestimmen, ob eine E-Mail Spam (oder Phish) enthält.

Sie können dazu beitragen, die Datenbanken zur Erkennung neuer Arten von Spam und Phish zu trainieren, indem Sie E-Mail-Muster an den SCM- oder MQM-Administrator senden. Ein einzelner McAfee Quarantäne-Manager kann das Training mehrerer SCM-Anwendungen übernehmen.

Mit dem Customer Submission Tool können Sie die Muster mit einem einzelnen Klick senden. Der Administrator kann entscheiden, welche Muster in die Datenbank eingereicht werden. Die Software analysiert den Inhalt jedes Musters, *lernt*, welche Phrasen für Spam typisch sind, und kann in Zukunft darauf zurückgreifen.

In gleicher Weise können Sie, wenn Sie E-Mails erhalten, die fälschlicherweise als Spam oder Phish kategorisiert wurden, diese E-Mails an den Administrator senden, damit sie für die Erkennung von Nicht-Spam verwendet werden.

Je mehr Muster korrekt eingereicht und für das Training verwendet werden, desto größer die Wahrscheinlichkeit, dass Spam und Phish in Zukunft korrekt kategorisiert werden können.

So funktioniert der Spam-Wert

Unsere Anti-Spam-Produkte wenden eine umfangreiche Reihe von Regeln auf jede E-Mail an. Jeder Regel ist ein Punktewert zugeteilt – positiv oder negativ. Regeln, die erfolgreich Charakteristiken von Spam erkennen, geben einen positiven Punktewert. Regeln, die erfolgreich Charakteristiken von wirklichen E-Mail-Nachrichten erkennen, geben einen negativen Punktewert. Die Punkte werden zusammengezählt, und jede E-Mail erhält einen *Spam-Wert*. Einige Regeln sind einfach und vergleichen nur mit allgemein verwendeten Phrasen. Andere Regeln sind komplexer und vergleichen die Informationen der Kopfzeile und die Struktur der E-Mails.

Anti-Spam-Produkte können eine Grenze festlegen, ab der eine E-Mail als Spam betrachtet wird. In der Regel zeigt ein Wert von 5 oder mehr an, dass eine E-Mail Spam ist. Ihr Anti-Spam-Produkt kann Nachrichten markieren, indem eine Textnachricht wie z. B. „**SPAM**“ in die Betreffzeile der E-Mail eingefügt wird. Sie können dann eine Spam-Mail einfach erkennen und entscheiden, wie Sie mit ihr umgehen wollen.

Es ist wichtig, dass Ihr Anti-Spam-Produkt richtig eingerichtet wurde, damit es Spam kategorisiert, wenn der Spam-Wert eine bestimmte Grenze überschreitet. Wenn der Wert zu hoch ist (ein Spam-Wert von 10 oder mehr), wird das Anti-Spam-Produkt einige Spam-Mails nicht erkennen. Wenn der Wert zu niedrig ist, werden einige wirkliche E-Mail-Nachrichten fälschlicherweise als Spam kategorisiert.

3 Installation des Tool

Für fortgeschrittene Benutzer und Administratoren

In diesem Abschnitt wird erklärt, wie das Customer Submission Tool Version 2.0 installiert wird. Außerdem enthält er die folgenden Informationen:

- *Installations-Checkliste* auf Seite 17
- *Herunterladen der Installationsdateien* auf Seite 18
- *Manuelle Installation des Tool* auf Seite 18
- *Installation des Tool mit einem Skript* auf Seite 19

Wenn Sie vorhaben, das Tool vielen E-Mail-Benutzern zukommen zu lassen, empfehlen wir, dass Sie ein Skript verwenden. Siehe *Installation des Tool mit einem Skript* auf Seite 19.

Installations-Checkliste

Wir stellen das Customer Submission Tool als Datei zum Download von unserer Website zur Verfügung. Bevor Sie das Customer Submission Tool installieren, lesen Sie die folgende Checkliste durch, und stellen Sie sicher, dass Ihr System so konfiguriert ist, dass das Installationsprogramm korrekt ausgeführt werden kann, und dass Sie über alle nötigen Informationen zur Installation des Programms verfügen.

✓ Der Computer verfügt über ein Betriebssystem Microsoft Windows 2000 (oder höher).

✓ Sie haben das aktuelle Servicepack für das Windows-Betriebssystem und Windows Updates installiert.

✓ Der Computer verfügt über einen Client Microsoft Outlook 2000 (oder höher). Das Customer Submission Tool kann nicht mit Microsoft Outlook Express oder anderen E-Mail-Clients verwendet werden.

✓ Der Computer hat Zugriff auf die Installationsdateien, die von der McAfee-Website heruntergeladen wurden.

✓ Sie verfügen über die administrativen Rechte und Berechtigungen, die zur Installation des Customer Submission Tool benötigt werden.

✓ Wenn Sie eine E-Mail an denMcAfee Quarantäne-Manager (MQM) senden wollen, benötigen Sie die folgenden Informationen:

- Name oder IP-Adresse des MQM-Servers, z. B. server1.domain1 oder 192.168.255.200. Sie können HTTP oder HTTPS oder das Protokoll verwenden.

Abhängig von Ihrem Authentifizierungsprozess benötigen Sie möglicherweise auch:

- Ihren Benutzernamen, um direkt auf MQM zugreifen zu können, z. B. netzwerkbenutzer@beispiel.de
- Ein Kennwort für den direkten Zugriff auf MQM.

✓ Wenn keine MQM-Software verfügbar ist, können Sie eine E-Mail an eine Secure Content Management (SCM)-Anwendung senden. Dazu benötigen Sie diese Informationen:

- Name oder IP-Adresse des SMTP-Servers, z. B. server1.domain1 oder 192.168.255.200.

  Es ist unwahrscheinlich, dass Sie von einer Workstation direkt auf die Anwendung zugreifen können; daher bezieht sich diese Adresse in der Regel auf das SMTP-Relay, das die E-Mails an eine SCM-Anwendung weiterleitet. Dies kann der Microsoft Exchange-Server sein.

- Nummer des SMTP-Serverports.
- E-Mail-Adresse für das Einsenden von nicht entdecktem Spam oder Phish.
- E-Mail-Adresse für das Einsenden von E-Mails, die fälschlicherweise als Spam oder Phish kategorisiert wurden.

Herunterladen der Installationsdateien

1 Erstellen Sie einen temporären Ordner auf Ihrer Festplatte.

2 Stellen Sie eine Verbindung mit dem Abschnitt über Anti-Spam-Produkte auf der McAfee-Website her: http://www.mcafeesecurity.com/us/products/mcafee/antispam/category.htm.

3 Suchen Sie den Abschnitt **Spam-Einsende-Tool** und extrahieren Sie den archivierten Ordner in dem temporären Ordner. Sie können die nötigen Hilfsprogramme zum Extrahieren von .ZIP-Archiven von den meisten elektronischen Services erhalten.

Manuelle Installation des Tool

Wenn Sie vorhaben, das Tool vielen E-Mail-Benutzern zukommen zu lassen, empfehlen wir, dass Sie ein Skript verwenden. Siehe Seite 19.

1 Schließen Sie alle Anwendungen.

2 Klicken Sie in dem temporären Ordner, in den Sie das Tool heruntergeladen haben, auf den Ordner **McAfee Customer Submission Tool**.

3 Suchen Sie die Datei MCST.EXE, und öffnen Sie sie, um den Installationsassistenten zu öffnen.

Wenn das Installationsprogramm nicht automatisch die richtige Sprache ausgewählt hat, öffnet sich ein Dialogfeld, in dem Sie eine Sprache auswählen können.

Abbildung 3-1 Dialogfeld „McAfee Customer Submission Tool Setup“

4 Klicken Sie auf **Weiter**, um die Seite **Zielordner** zu öffnen.

5 Klicken Sie auf **Durchsuchen**, um einen anderen Zielordner festzulegen, oder verwenden Sie den Standardordner. Klicken Sie auf **Weiter**.

6 Klicken Sie auf der Seite **Bereit zur Installation des Programms** auf **Weiter**, um die Seite **Systemaktualisierung** zu öffnen.

Die Seite zeigt Meldungen über den Fortschritt und eine Fortschrittsanzeige an. Die Dateien werden kopiert, und die Software wird installiert. Dies kann einige Minuten dauern. Wenn die Installation beendet ist, wird die Seite **McAfee Customer Submission Tool wurde erfolgreich installiert** angezeigt.

7 Klicken Sie auf **Beenden**, um den Assistenten zu schließen.

8 Starten Sie Microsoft Outlook. In der Standard-Symbolleiste von Microsoft Outlook sind zusätzliche Schaltflächen verfügbar. Siehe Abbildung 2-1 auf Seite 14.

Installation des Tool mit einem Skript

Wenn Sie vorhaben, das Customer Submission Tool auf mehreren Computern zu verwenden, empfehlen wir, dass Sie ein Skript verwenden. Informationen zum Download der benötigten Dateien finden Sie unter *Herunterladen der Installationsdateien* auf Seite 18.

Der Installationsbefehl hat im Allgemeinen die Form:

```
msiexec /qn /I mcst.msi Parameter1 Parameter2 Parameter3
```

Weitere Informationen über das Windows-Installationsprogramm finden Sie auf der Microsoft Website.

Alle Funktionen, die Sie einstellen können, wenn Sie das Tool manuell konfigurieren (wie beschrieben unter *Konfigurierung des Tool* auf Seite 28), können in diesem Befehl als Parameter spezifiziert werden.

Die folgenden Tabellen beschreiben die Parameter.

Tabelle 3-1 Allgemeine Parameter

Parameter und Standardwert		Beschreibung
CONFIGENABLED	1 (Ja)	Ermöglicht dem Benutzer die Konfiguration des Tool, indem die Schaltfläche **Einstellungen für das Einsenden konfigurieren** sichtbar gemacht wird. 0=Nein, 1 = Ja. Alle anderen Werte werden als 1 behandelt.
DELETESPAMONSUBMIT	0 (Nein)	Löscht alle Spam- (oder Phish-)Mails nach dem Einsenden. 0=Nein, 1 = Ja. Alle anderen Werte werden als 0 behandelt.
DONTSHOWSPAMSUBMIT	0 (Nein)	Zeigt das Dialogfeld „Einsenden“ nicht an, wenn der Benutzer auf die Schaltfläche zum Einsenden von Spam oder Phish klickt. 0=Nein, 1 = Ja. Alle anderen Werte werden als 0 behandelt.
DONTSHOWHAMSUBMIT	0 (Nein)	Zeigt das Dialogfeld „Einsenden“ nicht an, wenn der Benutzer auf die Schaltfläche zum Einsenden einer fälschlicherweise kategorisierten E-Mail klickt. 0=Nein, 1 = Ja. Alle anderen Werte werden als 0 behandelt.

Tabelle 3-1 Allgemeine Parameter (Fortsetzung)

Parameter und Standardwert		Beschreibung
INSTALLDIR1	Siehe Text.	Installiert das Tool an diesem Ort. Standardmäßig wird das Tool installiert in: „C:\Program Files\McAfee\Submission Tool“
MAXSUBMISSIONCOUNT	10000	Ermöglicht es dem Benutzer, bis zu 4 Milliarden Nachrichten gleichzeitig einzusenden. Alle Werte außerhalb dieser Spanne werden als 10000 behandelt.
REBOOT	(Keine)	Startet das Betriebssystem neu, nachdem die Installation abgeschlossen wurde. Mögliche Einstellungen sind F=Forcieren, S=Unterdrücken oder R=Wirklich unterdrücken. Wir empfehlen S oder R.

Tabelle 3-2 Parameter für das Einsenden an McAfee Labs

Parameter und Standardwert		Beschreibung
ASEENABLED	1 (Ja)	Aktiviert das Einsenden von Mustern an McAfee Labs.
ASERESPONSEFREQ	0 (Sofort)	Wie oft McAfee Labs auf die Einsendungen antwortet. Mögliche Einstellungen sind 0=**Sofort**, 1=**Täglich** oder 2=**Wöchentlich** oder 3=**Niemals**. Alle anderen Werte werden als 0 behandelt.
ASERESPONSETYPE	0 (Kurz)	Art der Bestätigung, die von McAfee Labs gesendet wird. Mögliche Einstellungen sind 0= **Kurz**, 1=**Normal** oder 2=**Detailliert**. Alle anderen Werte werden als 0 behandelt.

Tabelle 3-3 Parameter für das Einsenden an McAfee Quarantäne-Manager (MQM)

Parameter und Standardwert		Beschreibung
MQMENABLED	0 (Nein)	Aktiviert das Einsenden von Mustern an MQM. 0=Nein, 1 = Ja. Alle anderen Werte werden als 0 behandelt.
MQMPATH „http://mqm.beispiel.de/mqmuserui“		URL zum Ordner des Benutzers auf MQM.
WHITELISTHAMONSUBMIT	0 (Nein)	Fügt die Adresse des Absenders automatisch einer Weißen Liste hinzu, sofern die eingesendete E-Mail weder Spam noch Phish war. 0=Nein, 1 = Ja. Alle anderen Werte werden als 0 behandelt.
BLACKLISTSPAMONSUBMIT	0 (Nein)	Fügt die Adresse des Absenders automatisch einer Schwarzen Liste hinzu, sofern die eingesendete E-Mail Spam oder Phish war. 0=Nein, 1 = Ja. Alle anderen Werte werden als 0 behandelt.

Tabelle 3-4 Parameter für das Einsenden an Secure Content Management (SCM)

Parameter und Standardwert		Beschreibung
SCMENABLED	0 (Nein)	Aktiviert das Einsenden von Mustern an eine SCM-Anwendung. 0=Nein, 1 = Ja. Alle anderen Werte werden als 0 behandelt.
SCMRELAYSERVER	„mail.beispiel.de“	Name oder IP-Adresse des SMTP-Servers, z. B. server1.domain1 oder 192.168.255.200.
SCMRELAYPORT	25	Nummer des SMTP-Serverports. Die Spanne beträgt 1-65535.
SCMSPAMADRESS	„muster_spam@beispiel.de“	E-Mail-Adresse für das Einsenden von nicht entdecktem Spam oder Phish.
SCMHAMADRESS	„muster_keinspam@beispiel.de“	E-Mail-Adresse für das Einsenden von E-Mails, die fälschlicherweise als Spam oder Phish kategorisiert wurden.

Beispiele

Schließen Sie Zeichenfolgen in Anführungszeichen ein. Zum Beispiel:

```
INSTALLDIR1=„C:\FOLDER A\FOLDER 1“
```

Der folgende Befehl installiert im Hintergrund das Customer Submission Tool unter Verwendung der Standardwerte. Der Benutzer sieht lediglich die Schaltflächen **Spam-oder Phishing-Muster einsenden** und **Nicht-Spam-Muster einsenden** in der Symbolleiste von Microsoft Outlook. Nach Beendigung der Installation wird kein Neustart durchgeführt. Der Benutzer kann Muster nur an McAfee einsenden. Der Benutzer kann das Tool nicht neu konfigurieren.

```
msiexec /qn /i mcst.msi CONFIGENABLED=0 INSTALLDIR1=„C:\FOLDER A\FOLDER 1“ REBOOT=R
```

Der folgende Befehl installiert das Customer Submission Tool im Hintergrund, und ermöglicht es dem Benutzer, Muster an den McAfee Quarantäne-Manager einzusenden. Der Benutzer kann das Tool neu konfigurieren.

```
msiexec /qn /I mcst.msi MQMENABLED=1 MQMPATH=„http://mqm1/userui“ REBOOT=R
```

Der folgende Befehl installiert das Customer Submission Tool und ermöglicht es dem Benutzer, Muster an eine Secure Content Management-Anwendung zu senden. Der Benutzer sieht, wie die Installation durchgeführt wird. Der Benutzer kann das Tool neu konfigurieren.

```
msiexec /i mcst.msi SCMENABLED=1 SCMRELAYSERVER=„http://server1“ SCMRELAYPORT=1234
```

Einführung des Tool für E-Mail-Benutzer

Sie können eine Benachrichtigung an die E-Mail-Benutzer senden, wenn das Customer Submission Tool in ihre Microsoft Outlook-Clients installiert wurde.

Beispiel

Von heute an setzen wir das McAfee Spam-Einsende-Tool ein.

Durch das Tool werden wir die Menge an SPAM, die unsere Organisation erhält, reduzieren können. Zwei zusätzliche Schaltflächen werden in der Symbolleiste von Microsoft Outlook angezeigt. Wenn Sie die Schaltflächen (unten abgebildet) nicht sehen können, starten Sie Microsoft Outlook neu.

Klicken Sie auf diese Schaltfläche, um Muster von Spam einzusenden, die nicht als Spam entdeckt wurden:

Klicken Sie auf diese Schaltfläche, um Muster von E-Mail-Nachrichten einzusenden, die fälschlicherweise als Spam kategorisiert wurden:

Ändern der Konfigurierung

Um später einen Teil der Konfigurierung zu ändern, ohne das Tool erneut installieren zu müssen, können Sie die Registrierungseinstellungen bei folgendem Eintrag verändern:

HKEY_CURRENT_USER\Software\McAfee\Submission Tool

Die Einstellungen sind in der folgenden Tabelle aufgelistet:

Tabelle 3-5 Standard-Registrierungswerte

Name	Standardwert (hexadezimal)
AseEnabled	00000001
AseResponseFreq	00000000
AseResponseType	00000000
BlacklistSpamOnSubmit	00000000
ConfigEnabled	00000001
DeleteSpamOnSubmit	00000000
DontShowHamSubmit	00000000
DontShowSpamSubmit	00000000
MaxSubmissionCount	00002710
MqmEnabled	00000000
MqmPath	„http://mqm.beispiel.de/mqmuserui“
ScmDataTimeout	0000ea60
ScmEnabled	00000000
ScmHamAddress	„muster_keinspam@beispiel.de“
ScmRecvTimeout	0000ea60
ScmRelayPort	00000019
ScmRelayServer	„mail.beispiel.de“
ScmSendTimeout	0000ea60
ScmSpamAddress	„muster_spam@beispiel.de“
WhitelistHamOnSubmit	00000000

Die Namen in der Registrierung sind identisch zu den Parametern unter *Installation des Tool mit einem Skript* auf Seite 19.

Einige Namen, z. B. die SCM-Zeitüberschreitungen, sind nicht als Parameter verfügbar und können nur von der Registrierung aus eingestellt werden. Die SCM-Zeitüberschreitungen haben Standardwerte von 60.000 Millisekunden (1 Minute).

Um die veränderten Registrierungseinträge zu forcieren, starten Sie Microsoft Outlook neu. Wenn Sie inkorrekte Werte eingegeben haben, ersetzt das Tool sie mit den Standardwerten.

4 Verwendung des Tool

Schaltflächen und Menüeinträge

Nach der Installation werden durch das Customer Submission Tool in die Schaltfläche des Microsoft Outlook Client einige Schaltflächen und Menüeinträge hinzugefügt (siehe Abbildung 2-1 auf Seite 14). Dadurch stehen Ihnen folgende Aktionen zur Verfügung:

- Einsenden von E-Mails, die als Spam (oder Phish) hätten kategorisiert werden sollen. Siehe *Einsenden Ihres ersten Spam- oder Phishing-Musters* und *Einsenden weiterer Spam- oder Phishing-Muster auf Seite 25*.
- Einsenden von E-Mails, die fälschlicherweise als Spam (oder Phish) kategorisiert wurden. Siehe *Einsenden Ihres ersten falsch kategorisierten Musters auf Seite 26* und *Einsenden weiterer falsch kategorisierter Muster auf Seite 27*.
- Hinzufügen aller Ihrer Microsoft Outlook-Kontakte zu einer Weißen Liste (wenn McAfee Quarantäne-Manager verwendet wird). Siehe *Hinzufügen Ihrer Microsoft Outlook-Kontakte zur Weißen Liste* auf Seite 27.
- Konfigurieren einiger Tool-Einstellungen. Siehe *Konfigurierung des Tool* auf Seite 28.

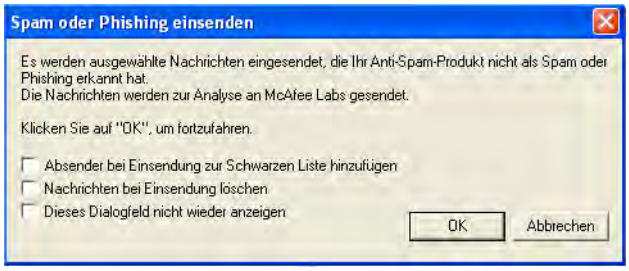
Einsenden Ihres ersten Spam- oder Phishing-Musters

Wenn Sie zum ersten Mal ein E-Mail-Muster einsenden, können Sie das Tool nach Belieben konfigurieren. So reichen Sie ein Spam- oder Phishing-Muster ein:

1 Öffnen Sie in Microsoft Outlook die E-Mail, oder wählen Sie die Betreffzeile der E-Mail aus.

2 Klicken Sie auf die Schaltfläche **Spam- oder Phishing-Muster einsenden** auf der Symbolleiste. Sie können auch das Menü **Aktion** verwenden. Ein Dialogfeld wird angezeigt:

Abbildung 4-1 Dialogfeld „Spam oder Phishing einsenden“



3 Wählen Sie im Dialogfeld die gewünschten Funktionen aus:

Funktion	Beschreibung
Absender bei Einsendung zur Schwarzen Liste hinzufügen	Dieses Kontrollkästchen ist nur verfügbar, wenn die Software McAfee Quarantäne-Manager verwendet wird. Absender der Spam-Mail zu einer Schwarzen Liste hinzufügen. In Zukunft wird jede E-Mail dieses Absenders blockiert werden.
Nachrichten nach Einsendung löschen	Löscht alle ausgewählten Spam- oder Phishing-Muster nach dem Einsenden.
Dieses Dialogfeld nicht wieder anzeigen	Dieses Dialogfeld wird in Zukunft nicht mehr angezeigt. In Zukunft können Sie dieses Dialogfeld anzeigen, indem Sie die Umschalttaste drücken und gleichzeitig auf die Schaltfläche **Spam- oder Phishing-Muster einsenden** klicken.

Klicken Sie auf **OK**, um das Dialogfeld zu schließen. Das Muster wird eingereicht.

4 Wenn Sie das Muster an den McAfee Quarantäne-Manager einsenden, müssen Sie Ihren Anmeldenamen und Ihr Kennwort eingeben.

5 Wenn eine Nachricht angezeigt wird, die besagt, dass das Muster erfolgreich eingereicht wurde, klicken Sie auf **OK**.

Das Tool reicht keine Muster ein, die zu groß sind (über 1MB), daher empfiehlt McAfee, dass Sie solche Dateien löschen.

Einsenden weiterer Spam- oder Phishing-Muster

So reichen Sie ein Spam- oder Phishing-Muster ein:

1 Öffnen Sie in Microsoft Outlook die E-Mail, oder wählen Sie die Betreffzeile der E-Mail aus.

Wenn Sie die Betreffzeilen der E-Mail anzeigen, können Sie mehr als ein Muster gleichzeitig einsenden. Verwenden Sie die UMSCHALTTASTE, um einen Block von E-Mails auszuwählen, die gleichzeitig eingesenden werden sollen. Verwenden Sie die STEUERUNGSTASTE, um mehrere einzelne Nachrichten auszuwählen.

2 Klicken Sie auf die Schaltfläche **Spam- oder Phishing-Muster einsenden** auf der Symbolleiste. Sie können auch das Menü **Aktion** verwenden.

Wählen Sie im Dialogfeld die gewünschten Funktionen aus: Siehe *Einsenden Ihres ersten Spam- oder Phishing-Musters* auf Seite 24. Wenn das Dialogfeld nicht angezeigt wird, können Sie es durch Drücken der UMSCHALTTASTE und gleichzeitiges Klicken anzeigen. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Das Muster wird eingereicht.

3 Wenn eine Nachricht angezeigt wird, die besagt, dass das Muster erfolgreich eingereicht wurde, klicken Sie auf **OK**.

Das Tool reicht keine Muster ein, die zu groß sind (über 1MB), daher empfiehlt McAfee, dass Sie solche Dateien löschen.

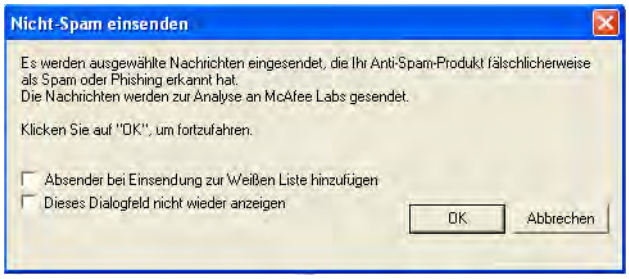
Einsenden Ihres ersten falsch kategorisierten Musters

Wenn Sie zum ersten Mal ein Muster einsenden, können Sie das Tool nach Belieben konfigurieren. So reichen Sie ein Muster ein, das fälschlicherweise als Spam oder Phish kategorisiert wurde:

1 Öffnen Sie in Microsoft Outlook die E-Mail, oder wählen Sie die Betreffzeile der E-Mail aus.

2 Klicken Sie auf die Schaltfläche **Nicht-Spam-Muster einsenden** auf der Symbolleiste. Sie können auch das Menü **Aktion** verwenden. Ein Dialogfeld wird angezeigt:

Abbildung 4-2 Dialogfeld „Nicht-Spam einsenden“



3 Wählen Sie im Dialogfeld die gewünschten Funktionen aus:

Funktion	Beschreibung
Absender bei Einsendung zur Weißen Liste hinzufügen	Dieses Kontrollkästchen ist nur verfügbar, wenn der McAfee Quarantäne-Manager verwendet wird. In Zukunft wird keine E-Mail dieses Absenders mehr als Spam kategorisiert.
Dieses Dialogfeld nicht wieder anzeigen	In Zukunft können Sie dieses Dialogfeld anzeigen, indem Sie die UMSCHALTTASTE drücken und gleichzeitig auf die Schaltfläche **Nicht-Spam-Muster einsenden** klicken.

4 Klicken Sie auf **OK**, um das Dialogfeld zu schließen. Das Muster wird eingereicht.

5 Wenn Sie das Muster an den McAfee Quarantäne-Manager einsenden, müssen Sie Ihren Anmeldenamen und Ihr Kennwort eingeben.

6 Wenn eine Nachricht angezeigt wird, die besagt, dass das Muster erfolgreich eingereicht wurde, klicken Sie auf **OK**.

Das Tool reicht keine Muster ein, die zu groß sind (über 1MB), daher empfiehlt McAfee, dass Sie solche Dateien löschen.

Einsenden weiterer falsch kategorisierter Muster

So reichen Sie ein Muster ein, das fälschlicherweise als Spam oder Phish kategorisiert wurde:

1 Öffnen Sie in Microsoft Outlook die E-Mail, oder wählen Sie die Betreffzeile der E-Mail aus.

> Wenn Sie die Betreffzeilen der E-Mail anzeigen, können Sie mehr als ein Muster gleichzeitig einsenden. Verwenden Sie die UMSCHALTTASTE, um einen Block von E-Mails auszuwählen, die gleichzeitig eingesendet werden sollen. Verwenden Sie die STRG-Taste, um mehrere einzelne Nachrichten auszuwählen.

2 Klicken Sie auf die Schaltfläche **Nicht-Spam-Muster einsenden** auf der Symbolleiste. Sie können auch das Menü **Aktion** verwenden.

   Wenn ein Dialogfeld angezeigt wird, wählen Sie die gewünschten Funktionen aus (wie in *Einsenden Ihres ersten falsch kategorisierten Musters auf Seite 26* beschrieben), und klicken Sie auf **OK**, um das Dialogfeld zu schließen. Wenn das Dialogfeld nicht angezeigt wird, können Sie es mit der Kombination UMSCHALTTASTE und Klicken anzeigen. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

   Das Muster wird eingereicht.

3 Wenn eine Nachricht angezeigt wird, die besagt, dass das Muster erfolgreich eingereicht wurde, klicken Sie auf **OK**.

Das Tool reicht keine Muster ein, die zu groß sind (über 1MB), daher empfiehlt McAfee, dass Sie solche Dateien löschen.

Hinzufügen Ihrer Microsoft Outlook-Kontakte zur Weißen Liste

> Diese Funktion ist nur verfügbar, wenn der McAfee Quarantäne-Manager installiert ist und das Customer Submission Tool so konfiguriert ist, dass die Schaltfläche **Einstellungen für das Einsenden konfigurieren** auf der Symbolleiste angezeigt wird.

Um zu verhindern, dass E-Mails Ihrer Microsoft Outlook-Kontakte als Spam (oder Phish) kategorisiert werden, können Sie die Adressen Ihrer Kontakte zu Ihrer Weißen Liste hinzufügen:

1 Klicken Sie in Microsoft Outlook auf die Schaltfläche **Einstellungen für das Einsenden konfigurieren** in der Symbolleiste.

2 Klicken Sie im **Customer Submission Tool** Dialogfeld auf **Kontaktadressen zur Weißen Liste hinzufügen**.

3 Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

In Zukunft werden E-Mails, die von einer der E-Mail-Adressen in Ihrer Weißen Liste gesendet wurden, nicht mehr auf Spam oder Phish überprüft. (Alle E-Mails werden auf Viren überprüft.)

Konfigurierung des Tool

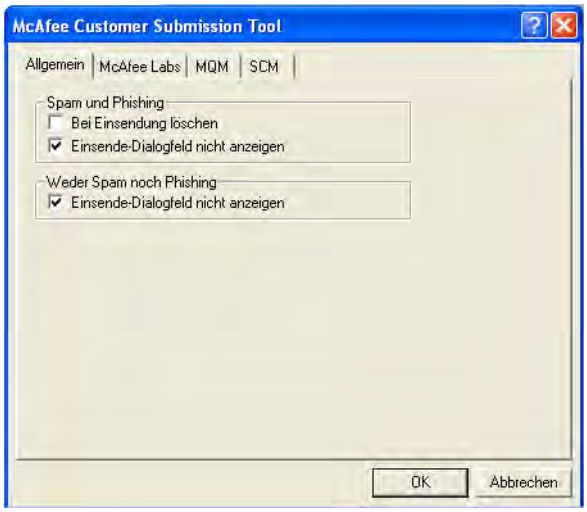
Wenn die Schaltfläche **Einstellungen für das Einsenden konfigurieren** in der Symbolleiste verfügbar ist, können Sie einige Funktionen des Customer Submission Tool konfigurieren. Diese Schaltfläche ist nur verfügbar, wenn die Betreffzeilen der E-Mails angezeigt werden.

Die Schaltfläche ist nicht verfügbar, wenn das Tool mit einem Skript installiert wurde, das diese Funktion nicht aktiviert hat.

So konfigurieren Sie das Tool:

1 Klicken Sie auf der Symbolleiste auf die Schaltfläche **Einstellungen für das Einsenden konfigurieren**. Ein Dialogfeld wird angezeigt:

Abbildung 4-3 Dialogfeld „McAfee Customer Submission Tool“



2 Wählen Sie im Dialogfeld die gewünschten Funktionen aus:

Bezeichnung	Beschreibung der Funktion
Bei Einsendung löschen	Löscht alle Spam- oder Phish-Mails nach dem erfolgreichen Einsenden.
Einsende-Dialogfeld nicht anzeigen	Es wird kein Dialogfeld mehr eingeblendet, wenn Spam-oder Phish-Mails (oder falsch kategorisierte E-Mails) eingereicht werden.

3 Wenn Sie Muster an McAfee Labs zur Analyse senden wollen, wählen Sie die Registerkarte **McAfee Labs** aus, klicken Sie auf **Aktivieren**, und stellen Sie dann die anderen Werte ein:

Bezeichnung	Beschreibung der Funktion
Häufigkeit der Antwort	Legen Sie fest, wie oft McAfee Labs eine automatische E-Mail zur Bestätigung Ihrer Einsendungen senden muss. Wenn Sie **Sofort** ausgewählt haben und mehrere Muster gleichzeitig einsenden, erhalten Sie möglicherweise mehrere Antworten in den nächsten Minuten.
Art der Antwort	Legen Sie fest, wie detailliert die automatischen E-Mails sein sollen. Zum Beispiel erhalten Sie bei der Einstellung **Kurz** nur eine Bestätigung.

Wenn Sie das Tool zum ersten Mal verwenden, empfiehlt McAfee, dass Sie die Einstellungen **Sofort** und **Kurz** festlegen.

4 Wenn Sie Muster an den McAfee Quarantäne-Manager einsenden wollen, wählen Sie die Registerkarte **MQM** aus, klicken Sie auf **Aktivieren**, und wählen Sie die Funktionen aus:

Bezeichnung	Beschreibung der Funktion
URL	Die Adresse des MQM-Servers im Format eines der folgenden Beispiele: ■ http://www.beispiel.de ■ 192.168.255.200
Benutzername	Der Benutzername (z. B. benutzer@beispiel.de), der bei der direkten Kommunikation mit MQM verwendet wird.
Kennwort	Das Kennwort, das dem Benutzernamen zugeordnet ist.
Adresse des Absenders nach dem Einsenden zur Schwarzen Liste hinzufügen.	In Zukunft wird jede E-Mail dieses Absenders blockiert werden.
Adresse des Absenders nach dem Einsenden zur Weißen Liste hinzufügen	In Zukunft wird keine E-Mail dieses Absenders mehr auf Spam oder Phish überprüft. E-Mails werden immer auf Viren überprüft.

5 Wenn Sie eine E-Mail an eine Secure Content Management-Anwendung einsenden wollen, wählen Sie die Registerkarte **SCM** aus, klicken Sie auf **Aktivieren**, und wählen Sie die Funktionen aus:

Bezeichnung	Beschreibung der Funktion
Server	Ein Servername im Format eines der folgenden Beispiele: ■ Server1 ■ 192.168.255.200 ■ mailto:192.168.255.200 ■ http://beispiel.de/benutzer ■ http://beispiel.de/benutzer:8080/benutzer1/ordner1
Port	Eine Portnummer, z. B. 25.
Spam und Phish	Eine Adresse (wie in der Anwendung konfiguriert), z. B. spam@beispiel.de.
Weder Spam noch Phish	Eine Adresse (wie in der Anwendung konfiguriert), z. B. keinspam@beispiel.de.

6 Klicken Sie auf **OK**, um das Dialogfeld zu schließen. Die neuen Einstellungen werden sofort übernommen.