



eSafe[®]

PROACTIVE CONTENT SECURITY

Proaktive Content Security für Internet Gateways und Mail Server

White Paper

Aladdin[®]

SECURING THE GLOBAL VILLAGE

A l a d d i n . d e

Dieses Schriftstück kann frei verbreitet werden, sofern gewährleistet wird, daß sein Inhalt nicht verändert, nicht gekürzt und alle Hinweise auf Handelsmarken beibehalten werden.

eSafe, eSafe Gateway und eSafe Mail sind Handelsmarken oder eingetragene Handelsmarken von Aladdin Knowledge Systems Inc.

Microsoft, Windows, Office und ActiveX sind Handelsmarken der Microsoft Corporation, FireWall-1, Check Point und das Check Point -Logo sind Handelsmarken oder eingetragene Markenzeichen der Check Point Technologies Ltd.,

Java ist eine Handelsmarke von Sun Microsystems Inc.

Alle anderen erwähnten Produktnamen sind Handelsmarken ihrer jeweiligen Inhaber.

Einführung	5
Firewalls sind nicht ausreichend	6
Proaktive Content Security	7
Die Gefahren	9
Was ist ein Virus?	11
Virustypen	11
Was ist ein Vandal?	12
Arten von Malicious Code	12
Wo sich Malicious Code versteckt	13
Warum digitale Signaturen nicht ausreichend sind	15
Weitere Gefahren aus dem Internet	16
Unangemessener und unproduktiver Inhalt	16
Missbrauch von Netzwerk-Ressourcen	16
Preisgabe sensibler Daten	16
eSafe Gateway	17
Technischer Überblick	18
Die fortschrittliche modulare TECS Architektur	18
Nahtlose Integration mit der Firewall-1	19
Einsatz in jeder Netzwerkumgebung	20
Kein Verlust an Bandbreite	20
Load-Sharing-Fähigkeit	21
Spezielllösung für Hochleistungs-Netzwerke	22
Vollständiger Gateway-Virusschutz	23
Kompletter Schutz vor Vandals	23
HTML-Vandals in Webseiten und eMails	23
Verhindern von Denial-of-Service-Angriffen	24
Schutz vor der Enthüllung von Daten und vor Spam	24
Schutz vor Mail-Relaying, Spoofing und Bombing	25
Schutz durch automatische Lernprozesse	25
Cookies, Skripts, Makros und Applet-Tags	25
Sperrern von unangemessenem Inhalt	26
Sichere Fernsteuerung	27
Kundenorientierte Systemanforderungen	28
Proaktives Aktualisieren	28
Anwenderrechte	29
eSafe Mail im Vergleich	30
eSafe Mail	31
Schutz vor Verbreitung sensibler Daten und Spam	31
Skalierbare Architektur mit hoher Verfügbarkeit	31
Flexible und mächtige Steuerung	31
Alarmmeldungen und Berichte	32
Halten Sie Trojanische Pferde und Viren von Ihrem Netz fern	32
eSafe Mail im Vergleich	33
Die eSafe Appliance	34
Vorteile im Einzelnen	35
Kompatibilität & Verfügbarkeit	36
Preise und Auszeichnungen	37
Über Aladdin	38

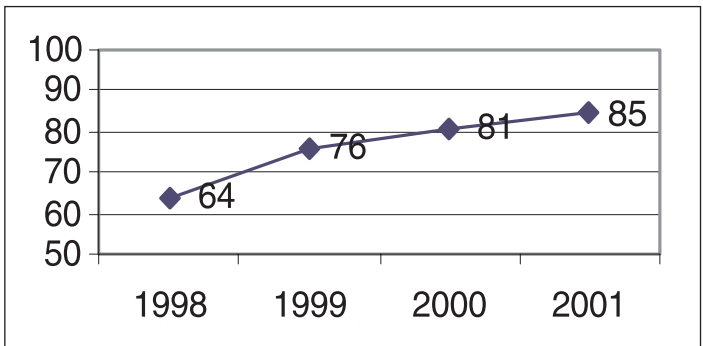
Einführung

Gefährliche Inhalte werden zur hauptsächlichen Ursache von Sicherheitslücken.

Die weite Verbreitung des Internets hat die Aufgabe, die Netzwerke zu schützen, komplizierter denn je gemacht. Firewalls und andere Schutzsysteme sind hervorragend geeignet, um unerwünschte oder gefährliche Verbindungen (zum Beispiel von Hackern zu unterbinden, bieten aber prinzipiell keinen Schutz gegen feindliche Inhalte. Tatsächlich steigen die Angriffe auf Computersysteme dramatisch an. Laut dem Computer Security Institute und dem FBI haben 2001 mehr als 80% der Firmen Erfahrung mit Sicherheitslücken im Computerbereich gemacht. Der geschätzte Schaden durch Viren erreichte laut "Computer Economics" im selben Jahr einen Rekordwert von 13 Milliarden US \$. So hat sich im Mai 2000 ein zerstörerischer Virus namens LoveLetter per eMail verbreitet, Millionen von PCs rund um die Welt binnen Stunden infiziert und geschätzte Schäden von über 7 Milliarden US \$ verursacht. NewLove und andere Mutationen folgten dem LoveLetter Vandal.

2001 verbreiteten sich CodeRed und Nimda. Sie wurden entwickelt, um Sicherheitslücken und Bugs in Betriebssystemen und Webserver-Applikationen auszuspionieren. Weltweit wurden Millionen Computer infiziert und mehr als 500.000 Webserver geknackt. Diese Art von Malicious Code verursachte schwere Schäden und rief tiefe Besorgnis über das Maß der Sicherheit von Internetinhalten hervor. Warum aber steigt die Zahl der geknackten Systeme, obwohl die Zahl der Unternehmen, die Firewalls oder andere konventionelle Antivirus-Produkte einsetzen, zunimmt?

Netzwerke mit Internet Sicherheitsstörungen in Prozent



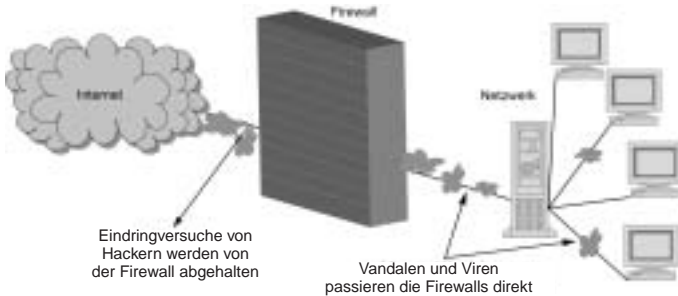
Quelle: CSI/FBI Computer Crime and Security Survey

Die Antwort ist einfach: Herkömmliches Hacken wurde um eine neue Form von Malicious Code erweitert. Gefährliche Inhalte wie Vandalen und Viren sowie unkontrollierte Übermittlung vertraulicher Informationen durch Angestellte sind auf dem Vormarsch.

Bevor wir erklären, wie eSafe Gateway und eSafe Mail Ihr Netzwerk sichern, ist es wichtig, die Grundsätze zu klären. Man wird feststellen, dass nicht nur die Datenbestände sondern auch die Ressourcen und Finanzen eines Unternehmens betroffen sind. Wir beginnen mit der Untersuchung der Arten von Sicherheitsrisiken, denen Netzwerke ausgesetzt sind, und zwar sowohl durch das Internet und eMail, als auch durch anderen Datenverkehr. Einige dieser Gefahren mögen bekannt sein (Viren), während andere relativ neu sind (Malicious Code).

Seit die Netzwerke der Unternehmen jeden Tag rund um die Uhr und von überall erreichbar sind, bauen nun die Organisationen auf Firewalls und implementieren damit Sicherheitsbarrieren, mit denen sie ihre Schnittstellen zum Internet schützen. Firewalls sind großartige Werkzeuge, um Netzwerke gegen Eindringversuche zu schützen. Dennoch bieten traditionelle Firewalls keine Mechanismen, die das Eindringen von Malicious Code, Viren und anderen schädlichen Inhalten in Computernetze verhindern. Schäden durch Verlust von geistigem Eigentum, Daten und durch gesetzliche Haftung sind die Folge.

Computernetz ohne Gateway Vandalen/Viren Schutz



Laut der neusten Untersuchung der "International Computer Security Association" (ICSA) über die Verbreitung von Viren, geschehen Zwischenfälle mit feindlichem Code jetzt in 98 % aller Organisationen, obwohl in 96 % davon Desktop-Antivirus-Programme verwendet werden. Das Internet bietet die Grundlage für die blitzartige Verbreitung von Viren und anderem feindlichem Code. Trotz des gestiegenen Einsatzes von Anti-Virus-Produkten auf Desktop-Computern, wuchsen die Schäden durch feindliche Programme in den letzten Jahren drastisch an: Der Grund dafür ist klar.

Der Angriffspunkt für feindliche Inhalte hat sich zu Internetgateways und Mailservern verlagert.

Obwohl die meisten Organisationen herkömmliche Anti-Virus-Software auf ihren Fileservern und Workstations einsetzen, lassen sie das Internetgateway völlig ungeschützt. Einmal in das System eingedrungen, umgeht der feindliche Inhalt die servergestützte Anti-Virus-Software, weil die Anwender die infizierten Dateien direkt auf ihre lokale Festplatte laden und von dort aus starten. Dabei ermöglicht der weitläufige Gebrauch von eMails eine weltweite Infektion mit Vandalen in wenigen Stunden. Schädliche Skripte in eMail-Anhängen, die zu zahlreichen Anwendern gesendet oder umgeleitet werden, infizieren daher sehr viele Desktop-Computer, ehe sie entdeckt werden. Diese Faktoren führten trotz weitverbreitetem Einsatz von Anti-Virus-Software zu steigenden Infektionszahlen.

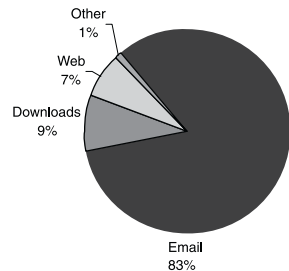
Web Seiten, die im HTTP Browsing-Protokoll eintreffen, werden überhaupt nur selten kontrolliert! HTML-Seiten sind aber bereits die Ursache für mehr als 7% aller Infektionen. Das bedeutet einen Zuwachs von 400 Prozent seit dem Jahr 2000 und bis jetzt wird dieser Bereich nicht durch konventionelle Anti-Virus-Lösungen geprüft. Eine vollständige HTML-Prüfung ist so kompliziert, dass diese Aufgabe nur durch eine hochspezialisierte Anwendung erledigt werden kann.

Firewalls sind nicht ausreichend

Die meisten Vandalen/Viren werden heute über das Internet übermittelt.

Firewalls können Hacker blockieren, stoppen aber nicht unfriendly Programme oder unangemessene Inhalte.

Ursprünge des Malicious Code
Quelle: ICSA Survey 2001



Proaktive Content Security

Gatewayschutz gegen feindliche Inhalte ist die kostengünstigste Strategie.

Das Warten auf einen Angriff ist ein reaktives Verhalten, und so verfahren die meisten Antivirus-Lösungen. Täglich werden neue Viren, Malicious Code, Trojanische Pferde und Würmer entwickelt und diese können in wenigen Stunden über die ganze Welt verstreut werden. Feindliche Skripte, die in Webseiten eingebettet sind und sogar HTML formatierte eMails, Anhänge, Java und ActiveX-Controls erfordern einen neuen, fortschrittlichen und proaktiven Ansatz.

Das Geheimnis einer wirksamen Content Security Lösung ist, den Malicious Code aufzuhalten, bevor er Ihr Unternehmensnetzwerk erreicht. Proaktive Lösungen wie eSafe Gateway und Mail, stellen sicher, dass die Gefahr gebannt wird, bevor sie eintritt ohne dass Arbeitszeit verschwendet wird und Ressourcen nicht vergeudet werden. Ihr Unternehmen spart dadurch Tausende Euro für teure Reparaturen und wertvolle Zeit. Die fortschrittlichen Management-Instrumente gewährleisten Ihnen die volle Kontrolle und versetzen sie in die Lage, einen Internet Sicherheitsplan umzusetzen, Spam zu reduzieren, eMail Spoofing und Bombing zu verhindern und die Webnutzung zu kontrollieren.

ROI-Annahmen

Bei der Berechnung der Kapitalrendite (ROI), setzen wir die Gesamtkosten einschließlich der Kosten für die Erkennung, das „Cleaning“ und den Produktionsverlust, multipliziert mit der Anzahl der schlimmsten Unfälle in einem Jahr an. Die Vorteile des Gateway-Schutzes liegen hier klar auf der Hand. Das folgende Beispiel stellt die Gesamtkosten für die Ausfallzeit, die Preisfestsetzung und den Produktionsverlust während eines einzigen Befalls in einer Organisation von 1000 Anwendern dar. Diese Rechnung schließt nicht den Betrag für die Kosten ein, die durch den Verlust von Daten- und Informationssicherheit entstehen.

* Für 2001 berichteten die ICSA-Überwachungsfachleute von durchschnittlichen Kosten in der Höhe von \$ 120.000.- pro Unfall. Die Kosten lagen bei \$ 10.000.- bis über \$ 1.000.000.-. Weitere Informationen über die ICSA finden Sie unter www.isca.net.

Die Kosten für die eSafe Gateway Lizenz für 1000 Anwender können durch eine 100prozentige Kapitalrendite beim ersten verhinderten Unfall abgedeckt werden.

Ohne Internet Gatewayschutz	
Ein einziger Unfall ohne den proaktiven Gateway-Schutz bei 1000 Angestellten, von denen jeder durchschnittlich 30 Minuten Stillstandszeit hat, in der er nicht arbeiten kann (basiert auf \$ 40/Stunde)	1000x\$20 = \$20,000
produziert Kosten, und für die IT-Spezialisten (basiert auf \$80/Std. und 3 Minuten durchschnittliche Zeit pro User)	1000x\$4 = \$4,000
es entstehen Gesamtkosten für einen einzigen Virus/Vandal-Unfall von	\$24,000

Wenn der Gateway-Schutz installiert ist, wird die Datei gesäubert, bevor sie in das Netzwerk kommt oder in der Mailbox des Anwenders auf dem Mailserver eintrifft. Eine so entschärfte Datei verhält sich genau wie jede andere saubere Datei und die Arbeit geht ohne Unterbrechung weiter. Wenn proaktive Methoden am Gateway eingesetzt werden, können vollständig neue, bisher unbekannte schädliche Codes aufgehalten werden, bevor sie aktiv werden oder passende konventionelle Antivirus-Programme im Handel sind.

Ein Desktopschutz wird aber immer dennoch benötigt. Es ist wichtig zu betonen, dass ein guter Gatewayschutz einen guten Desktopschutz gegen Viren und Vandalen nicht überflüssig macht. Viele Hackerseiten, oder von Hackern gekrackte und veränderte Seiten, können verschlüsselte HTML-Seiten enthalten (z.B. unter Verwendung von SSL). Diese Seiten können nur mit einer Desktop-Browser-Applikation geöffnet werden. Deswegen kann keine Gateway-Applikation diesen Inhalt prüfen. Daneben kann ein schädlicher Code auch über andere Wege, z.B. über Modem-Verbindungen oder infizierte Dateien, die im Netzwerk, auf CD-ROMs, ZIP-Laufwerken, Disketten oder anderen beweglichen Medien gespeichert sind, ihren Computer infizieren. Externe Mitarbeiter benutzen häufig Laptops und greifen von verschiedenen Standpunkten auf Dateien und Internetinhalte zu, ohne Firewalls oder andere Gateway-Schutzprogramme zu passieren. eSafe stellt somit der Organisation einen **vielschichtigen, proaktiven** Schutz gegen bekannte und unbekannte Gefahren zur Verfügung.

Gateway-Schutz kann Antivirensoftware für den Einzelplatz nicht ersetzen.

Die Gefahren

Die meisten Netzwerke sind vollkommen ungeschützt gegen Java-, ActiveX- und Script Vandalen.

E-Mail wird oft zur unbefugten Übermittlung von Informationen gebraucht.

Aus einer Umfrage von IDC: „Wie oft surfen Sie auf Seiten, die nicht mit der Arbeit zu tun haben?“ Antwort:

32,86% - Mehrmals täglich;

20,11% - Mehrmals wöchentlich;

37,11% - Ständig;

9,92% - Niemals!

Die Gefahren durch Internet-Vandalen sind extrem hoch. Vandalen können gegen bestimmte Firmen gerichtet sein. Anders als Viren richten sie unverzüglich Schäden an. Um die Sache noch schlimmer zu machen, sind heute die führenden Antivirenpakete nicht in der Lage, die meisten Vandalen aufzuspüren. In der Vergangenheit haben manche Netzwerkadministratoren versucht, dieses Sicherheitsrisiko zu verringern, indem sie Java und ActiveX gänzlich blockiert haben. Dieser Ansatz ist aber heutzutage nicht mehr geeignet, da diese aktiven Technologien für die Funktion und volle Effizienz mancher Websites unentbehrlich geworden sind.

Unproduktive und unangemessene Inhalte. Unproduktiv ist jeder ablenkende Inhalt, der laut den Unternehmensrichtlinien nichts mit der Arbeit zu tun hat. Das umfasst Spam und Websites mit Themen wie z.B. Glücksspiel, Reisen, Sport, Erotik, Rassismus usw. Manche Untersuchungen veranschlagen, dass 75% des Websurfing am Arbeitsplatz geschieht. Entgegen der Vorschriften verbringen Angestellte oft wertvolle Zeit und nutzen teure Bandbreite mit dem Besuch unproduktiver Sites. Zudem gibt es Hunderte von Webseiten, die Sammlungen von Hackertools und feindlichen Code bereitstellen. Angestellte mit bössartigen Absichten benutzen oft diese Toolsammlungen. Angestellte können aber auch unbeabsichtigt zum "Hacker" werden wenn sie unbewusst solche Tools verwenden. Das lokale Netzwerk kann so infiziert und oft vollkommen für die Außenwelt zugänglich gemacht werden.

Spam-Mails. Spam, auch beschrieben als unverlangt gesandte MasseneMail oder "Müll"-eMail, ist unerwünschte elektronische Post, die an zahlreiche Empfänger verschickt wird, und zwar mit der Absicht für ein Geschäft, eine Idee oder einen Dienst zu werben. Spam wirbt gewöhnlich mit "werden Sie schnell reich", für Systeme, Pornoseiten, Reise- und Urlaubsservices und eine Vielzahl anderer Themenbereiche. Hacker benutzen außerdem Spam, um Viren und Malicious Code per eMail zu verbreiten und Anwender durch Tricks dazu zu bringen, gehackte oder feindliche Seiten zu besuchen, die dann unbedarfte Surfer angreifen.

Mail-Spoofing. Mail-Spoofing bedeutet, die Fälschung des Absenders einer eMail. Das kann gefährlich werden, wenn sich jemand für einen anderen ausgibt. Hacker und Spammer machen ausgiebig Gebrauch davon.

Mail-Relaying. Mail-Relaying bedeutet, dass jemand von außerhalb ihrer Organisation ihren Mailserver dazu benutzt, um eMails an Dritte zu übertragen. Hacker benutzen diese Technik für das Mail-Spoofing oder Denial of Service-Attaken (DoS), gegen Mailserver Dritter. Mail-Relaying überlastet unnötigerweise den davon betroffenen Mailserver und kann rechtliche Probleme zur Folge haben.

Mail-Bomb. Mail-Bomb-Angriffe sind DoS Angriffe, bei denen ein Mailserver mit Tausenden von falschen eMails überflutet wird, damit dieser Server stehen bleibt oder zusammenbricht.

Bloßstellung von Daten. Ein eMail-Anschluß schafft die Möglichkeit schnell an die benötigten Informationen zu kommen. Genauso können aber nicht freigegebene, vertrauliche Informationen weltweit und blitzschnell übermittelt werden. Organisationen sind für die Handlungen ihrer Angestellten verantwortlich

und der eMail-Verkehr stellt einen Kanal dar, der oft für illegale oder unproduktive Aktivitäten benutzt wird. Angestellte benutzen firmeneigene eMail-Anschlüsse, um vertrauliche Projekte, Geschäftsstrategien und private Kundendaten zu verraten sowie um Nebentätigkeiten nachzugehen. Abgesehen davon, dass dadurch kostbare Bandbreite verloren wird, haften die Organisationen rechtlich für diese Aktivitäten.

Die Lösung ist offensichtlich. Um von den Möglichkeiten des Internet profitieren zu können, ist zugleich auch eine umfassende und proaktive Schutzeinrichtung nötig. Am Eingang zum Netzwerk muss deshalb ein Schutz vor bösartigen Inhalten installiert werden. Dieser Eingang ist am Gateway, parallel zur Firewall, und am Mailserver.

Die folgende Tabelle zeigt die Unterschiede zwischen bösartigen Programmen 1987 (als der erste Virus entdeckt wurde) und dem Jahr 2000. Sie zeigt deutlich, dass es heute nahezu unmöglich ist, innerhalb von 5 Stunden für eine weltweite Infektion, traditionelle Virenupdates zu Verfügung zu stellen.

Vandal/Virus	Jahr der Entdeckung	Typ	Verbreitungszeit	Schaden ca.
Jerusalem	1987	.exe Dateivirus	5 Jahre	50 Mio. \$
Cascade	1990	Bootsektorvirus	3 Jahre	50 Mio. \$
Concept (erster Macrovirus)	1995	Word Makrovirus	4 Monate	50 Mio. \$
Melissa	1999	Emailfähiger Word Makrovirus	4 Tage	93 – 385 Mio. \$
I Love You (auch LoveBug oder loveletter)	2000	Emailfähiger VBScript Vandal	5 Stunden	7 Mrd. \$

*Quelle: ICSA, www.icsa.net

Was ist ein Virus?

Ein Computervirus ist ein Programm, das andere Programme befällt, indem es eine (möglicherweise weiterentwickelte) Kopie seiner selbst an sie anhängt. Er ist nicht unbedingt dazu gedacht, Schaden zu verursachen, tut es aber oft. Viren werden von Computer zu Computer übertragen, wenn der Benutzer befallene Programme ausführt oder befallene Dateien öffnet. Laut der "International Computer Security Association" verbreitet sich diese Art von Malicious Code schneller als sie gestoppt werden kann. Die einzige Lösung ist, die Unternehmen zu schulen und einen automatischen, permanenten Virenschutz gegen bekannte und unbekannte Viren zu installieren.

Virustypen

Viren haben verschiedene Gemeinsamkeiten: sie brauchen ein ausführbares "Wirtsprogramm", sie vermehren sich und können durch Signaturscanning aufgespürt werden. Viren können in verschiedene Kategorien eingeteilt werden:

- **Dateiviren** hängen sich an normale Programmdateien an. Sie befallen normalerweise .COM- und/oder .EXE-Dateien. Manche befallen aber auch andere Dateien mit ausführbarem Code, wie .SYS-, .OVL-, .DLL- und .PRG-Dateien. Die Mehrzahl der Dateiviren versteckt sich irgendwo im Speicher, wenn das befallene Programm erstmalig ausgeführt wird und infizieren dann alle nachfolgend aufgerufenen Programme. Manche werden auch als polymorphe Viren beschrieben, die veränderte Kopien von sich erstellen (meist durch Selbstverschlüsselung mit veränderlichem Schlüssel).
- **Systemdateiviren** sind Viren, die die Einträge in den Verzeichnissen ändern, so dass der Virus vor dem gewünschten Programm geladen wird. Das Programm wird nicht verändert, nur sein Platz im Verzeichnis.
- **Makroviren** befallen Microsoft Office Dokumente (wie Word und Excel). Sie sind in Scriptsprache oder Visual Basic geschrieben und besitzen noch mehr Zerstörungskraft. Diese Viren sind für die Mehrzahl der Vireninfektionen verantwortlich. Makroviren können Wörter in Dokumenten vertauschen, Farben ändern, die Festplatte formatieren, Dokumente ohne Wissen des Anwenders per eMail verschicken, sich per Microsoft Outlook verbreiten und mehr.
- **System/Bootrecord Viren** befallen den ausführbaren Code, der sich in bestimmten Bereichen einer Festplatte befindet, die nicht zum gewöhnlichen Speicher gehören. Einige Viren verändern auch die CMOS Einstellungen. Der CMOS-Speicher befindet sich jedoch nicht im normalen Adressbereich der CPU und kann nicht ausgeführt werden. Daher kann ein Virus die CMOS-Information beschädigen und verändern, sich dort aber nicht verstecken.

Weitere Informationsquellen:
NIST Virus Research Center : http://csrc.nist.gov/virus/
Rob Rosenberger's Computer Virus Myths Page: http://www.vmyths.com/
In the Wild Organization: http://www.wildlist.org

Was ist ein Vandale?

Vandalen werden von Antivirensoftware und Firewalls allein nicht aufgehalten.

Der „I Love You“ Vandale verursachte 9 Mrd. \$ Schaden in nur fünf Tagen.

Im Unterschied zu einem Virus ist Malicious Code eine selbstausführende Internetanwendung, die nicht durch Antivirensoftware und Firewalls allein blockiert werden kann. Normalerweise reproduzieren sie sich nicht, wenn sie Dateien infizieren (wie Viren), sondern sie verursachen vielmehr augenblickliche Schäden. Anders als bei Viren, hat sich die volle Zerstörungskraft schon entfaltet, wenn der Malicious Code identifiziert wird.

Seine Beschaffenheit macht den Malicious Code zu einem idealen Werkzeug für Leute, die ein bestimmtes Netz oder eine Firma treffen wollen. Jeder kann einen Vandal an eine eMail anhängen oder auf einer von den Angestellten einer Firma besuchten Seite unterbringen.

Programmierer mit feindlichen Absichten benutzen Malicious Code, um Zugang zu Dateien in Netzwerken zu bekommen, selbst wenn diese durch Firewalls geschützt sind. Im Frühjahr 1997 hat eine deutsche Hackerorganisation einen ActiveX-Code benutzt, um Quicken-Daten von den Festplatten von denjenigen Usern zu stehlen, die die Webseite der Organisation besuchten. Seitdem wurde von Hunderten von Vandal-Angriffen berichtet.

Ein aktuelles Beispiel für die Durchschlagskraft und Verbreitungsgeschwindigkeit von Malicious Code zeigt der LoveLetter-Vandal-Ausbruch vom Mai 2000. Ein philippinischer Student erfand "LoveLetter", er wurde in VBScript geschrieben und erreichte die Opfer als eMail-Anhang. Als Verbreitungsmechanismus wurden die Windows Mailfunktionen benutzt. Nach dem Befehl verschickte sich dieser Malicious Code an alle Adressen aus dem Adressbuch weiter. Er benutzte einen psychologischen Trick, damit die Empfänger die eMail öffneten. Der Absender war dem Opfer bekannt und die Botschaft war "Ich liebe Dich". Die angehängte Datei war scheinbar ein Liebesbrief. Millionen von Anwendern wurden befallen - binnen fünf Stunden vorbereitet sich der Malicious Code weltweit. Die Schäden summierten sich in fünf Tagen auf geschätzte 7 Mrd. US \$. Innerhalb weniger Tage gab es Duzende von Varianten, mit einer Zerstörungskraft, die vom Zeigen einiger Meldungen bis hin zur Zerstörung von Dateien und sogar Passwort-stehlenden Trojanern reichte.

Arten von Malicious Code

Java - Diese Programme sind Applets, die geschaffen sind, um von Internet Clients ausgeführt zu werden, die wie die meisten modernen Browser eine "Virtual Java Machine" enthalten. Obwohl Java-Script (wurde von Sun Microsystems entwickelt) selbst über einige eingebaute Sicherheits-Features verfügt, werden derzeit auch Applets von der "Java Virtual Machine" interpretiert die nicht von Sun entwickelt worden sind. Deswegen sind Hunderte von Applets geschrieben worden, die trotz der Sicherheitsmaßnahmen in der Java-Sprache schwerwiegende Sicherheitsprobleme darstellen. Diese Applets können Denial-of-Service- (DoS) Angriffe auslösen, nicht freigegebene Dateien öffnen, Passwörter stehlen oder Systemressourcen von Anwendern stehlen, die eine Website besuchen. Diese Programme werden automatisch beim Besuchen einer Site installiert bzw. ausgeführt und können unmittelbar Schaden anrichten.

ActiveX - Diese Programme sind entwickelt worden, um auf Internetclients - normalerweise der Internet Explorer - ausgeführt zu werden, die ActiveX unterstützen. Anders als für Java gibt es für diese Programme keine Standardsprache. Sie können in verschiedenen Programmiersprachen geschrieben und vom Entwickler compiled werden und kommen beim Client als Binär-Code an. ActiveX hat keine eingebauten Sicherheitscodes und ActiveX-Objekte können alles, was sich der Entwickler vorstellen kann. Sich an Außenstehende ver-

schicken, den Computer sofort abschalten, Denial-of-Service-Angriffe starten, Modems neu wählen lassen, Daten löschen, Festplatten formatieren und vieles mehr. Diese Programme werden automatisch von der besuchten Site installiert bzw. ausgeführt und richten unmittelbar Schaden an.

Scripts - Diese Programme können in den HTML-Code einer Web-Seite eingebaut, als eMail-Anhänge verschickt oder sogar in eine HTML-formatierte eMail eingebunden werden. Sie können auch mit einer Vielzahl von Applikationen verwendet werden, die ihre Syntax unterstützen. Eine solche Applikation ist Windows Scripting Host, ein Automatisierungstool das hauptsächlich vom Malicious Code ausgenutzt wird. Scripts können fast alles - ein System mit Trojanischen Pferden infizieren, Dateien verändern, Denial-of-Service-Angriffe (DoS) auslösen oder feindliche Codes über das Netzwerk unter Ausnutzung von Microsoft Outlook oder Outlook Express, IRC (Chat-Anwendungen) und Instant Messengers, wie MSN-Messenger, verbreiten. Scripts werden in VBScript, JavaScript, JScript oder anderen Scriptsprachen geschrieben.

Cookies - Cookies sind Textdateien, die beim Besuch einer Seite auf die lokale Festplatte der Anwender geschrieben werden. Sie werden von einer Web-Site benutzt, um Informationen über die Aktivitäten des Anwenders auf seiner Festplatte zu speichern, und damit Platz auf dem Webserver zu sparen. Beispiele der in Cookies gespeicherten Informationen sind Kaufgewohnheiten, Lieblingsthemen, Passwörter für geschützte Web-Sites und Userprofile. Da Cookies keinen ausführbaren Code besitzen, können sie selbst keinen Angriff starten. Dennoch speichern sie vertrauliche Informationen, die von anderen Websites mittels Scripts oder ActiveX ausgelesen werden können. Diese vertraulichen Informationen können benutzt werden, um eMails zu fälschen, Zugangscodes zu stehlen und die Gewohnheiten des Anwenders kennenzulernen.

Wo sich Malicious Code versteckt

eMail - Die Verwendung von eMails ist heutzutage sehr verbreitet. Zusätzlich zum Text kann eine eMail alle möglichen Anhänge enthalten, wie auch präparierte Shortcuts und Malicious Code. eMail-Anhänge können Vandalen, Trojanische Pferde oder Viren enthalten. Jeder kann eMails mit feindlichen Anhängen oder Inhalten erhalten oder versenden ohne zu wissen, dass er angegriffen worden ist. Ohne Schutz hat der infizierte Anhang Zugang zu allen Dateien im gesamten Netz.

Webcontent - Surfen ist die zweitpopulärste Aktivität im Internet und dabei die Unsicherste. Die neusten Internet-Technologien, besonders Java und ActiveX, werden zur Erstellung von dynamischen, inhaltsorientierten Seiten benutzt. Unglücklicherweise bergen diese neuen Technologien auch das höchste Risiko. Java Applets und ActiveX Controls werden durch simples Ansehen einer Website heruntergeladen und ausgeführt. Durch das Ansehen der Seite erlaubt der Anwender der Webseite, ein unbekanntes Programm ins Netzwerk zu kopieren und auszuführen. Es ist möglich den Web-Browser so zu konfigurieren, dass keinerlei Java- oder ActiveX-Inhalte heruntergeladen werden, jedoch ist das zunehmend weniger praktikabel, da viele Webseiten diese Technologien für eine volle Funktionalität verlangen.

"Vertrauenswürdige" Seiten - Die Tatsache, dass der Anwender eine "vertrauenswürdige" Seite betrachtet, bedeutet nicht, dass diese nicht von Vandalprogrammen verändert worden sein könnte. Jedes Jahr werden Tausende von Web-Seiten gehackt. Hacker greifen oft traditionelle Bastionen der Sicherheit nur wegen der Herausforderung an. Wenn jemand den Text oder die Grafik verändern kann, kann er auch ein Vandalprogramm anbringen, um Daten zu beschädigen oder zu stehlen.

Dateidownloads - Obwohl die Datenübertragung sehr häufig im Internet erfolgt, und viele der oben beschriebenen Risiken birgt, stellt sie eine kleinere Gefahr dar, da sie gewöhnlich von erfahrenen Anwendern durchgeführt wird. Dennoch, kann der Anwender, indem er einer Produktbeschreibung glaubt, versehentlich ein Programm herunterladen, das sich bei seiner Ausführung anders verhält, als erwartet.

Weitere Informationen:
Princeton University Secure Internet Programming Page:
http://www.cs.princeton.edu/sip/
Demonstration von Beispielen von Vandal-Angriffen
http://www.ealaddin.com/home/csrt/demo
The Java Security Hotlist: http://www.cigital.com/javasecurity/
Listen von verunstalteten Websites: http://www.attrition.org/mirror/attrition/

Warum Digitale Signaturen nicht ausrei- chend sind

Digitale Signaturen bieten keine 100%-ige Sicherheitsgarantie.

Einige Produkte haben eingebaute Kontrollmechanismen für digitale Signaturen, um unsignierte Java- und ActiveX-Controls auszuschließen. Teilweise versagt diese Kontrolle, wenn es um den Ausschluss von Malicious Code geht.

Sowohl Microsoft (für die eigene ActiveX-Technologie) als auch Sun (für die Java Sprache) haben behauptet, dass eine signierte, selbstausführende Anwendung kein Malicious Code sein kann. Der Schlüssel für die digitale Signatur wird von einer Certification Authority (CA) ausgegeben.

Der gesamte Zertifizierungsprozess lässt einige Sicherheitsgrundsätze vermissen. Selbst wenn die Zertifizierungsbehörde ihre Arbeit tut und den Antragsteller identifiziert, kann dieser der Behörde immer noch eine falsche Identität liefern. Noch gravierender ist es, dass absolut nichts getan wird, um festzustellen, ob die Anwendung feindlich ist. Durchschlagende Beweise finden sie für ActiveX Control unter:

<http://www.ealaddin.com/home/csrt/demo/all/docpirate.asp>

Dieses signierte ActiveX-Control stiehlt das jüngste Worddokument im Ordner "Eigene Dateien". Das entsprechende Zertifikat sehen Sie unten.



Also garantiert die Zertifizierung für nichts, auf keinen Fall für die Wirkung oder Absicht des Codes. Sie versucht lediglich, dem Anwender zu zeigen, wer das Applet oder Control geschrieben hat, so dass er entscheiden kann, ob er dem Autor vertraut oder nicht. Die meisten Anwender klicken bei allen Warnhinweisen automatisch auf "fortfahren" und akzeptieren alle Applets und Controls, ohne die Konsequenzen zu beachten. Es gab auch Fälle von gestohlenen legitimierten Zertifikaten, mit denen gefährliche ActiveX-Codes signiert worden waren.

Wenn Sie ein Päckchen mit der Post erhalten, können Sie nicht sicher sein, das es keine Bombe enthält, nur weil der Absender eine Retouradresse und eine Briefmarke angebracht hat. Das bedeutet nur, dass der Empfänger nach der Explosion herausfinden könnte, wer der Verantwortliche ist, vorausgesetzt er hat seine richtige Adresse auf das Päckchen geschrieben. Genau so verhält es sich mit Internetinhalten: Nur eine gründliche Untersuchung, die unabhängig von digitalen Signaturen durchgeführt wird, bietet eindeutig den einzig sicheren Schutz gegen Malicious Code.

Unangemessener und unproduktiver Inhalt

Zusätzlich zum Besuch von unangemessenen und unproduktiven Web-Sites während der Arbeitszeit, könnten einige Angestellte auch noch ihre Internetprivilegien für illegale und andere unproduktive Tätigkeiten missbrauchen, wie zum Beispiel für Nebentätigkeiten. Abgesehen davon, dass sie teure Bandbreite kosten, haften Organisationen rechtlich für diese Aktivitäten und wachsende Ausgaben.

Missbrauch von Netzwerk-Ressourcen

Die Verbindung ins Internet kann sehr kostspielig sein; die ISP-Verbindungskosten wachsen entsprechend den angeforderten Bandbreiten. Die steigende Popularität von Unterhaltungsprogrammen im Internet, insbesondere Musik und Videos, stellen eine Herausforderung für die Administratoren dar. Der Download solcher Dateien fordert eine erhebliche Bandbreite und große Speicherplätze. Wenn auch Streaming-Dateien (Dateien, die kein Download erforderlich machen, sondern "live" vom Quellserver abgespielt werden) keinen Speicherplatz belegen, so binden sie doch eine wichtige Bandbreite und schränken den Service drastisch ein. Auch der Empfang von umfangreichen Dateien als eMail-Anhänge kann erheblichen Speicherplatz verschwenden. Die meisten Websites, die beanstandet werden können, beinhalten solches "Bandbreitenfresser-Material" wie z.B.:

- Pornographische Filme oder Bilder - ein Film kann eine Größe von 3 bis 700 MB haben;
- Kopien von Film- oder TV-Programmen - hier ist jeder Film oder jedes TV-Programm ein Download von ca. 300-650 MB;
- Clipart-Bilder oder Spielen - jede CD mit Bildern bedeutet einen Download von 500-700 MB
- Songs im MP3-Format - jeder Song bedeutet ein Download von 3,5-8 MB.

Diese Daten beanspruchen nicht nur einen erheblichen Teil der zur Verfügung stehenden Bandbreite sondern stellen auch ein rechtliches Problem dar, weil davon ausgegangen werden kann, dass es sich um illegales Material handelt, das gegen die Urheberrechte verstößt oder auch hoch kriminelle und gefährliche Inhalte, wie Kinderpornographie, Kindesmissbrauch oder die Darstellung extremer Gewalt, birgt.

Preisgabe sensibler Daten

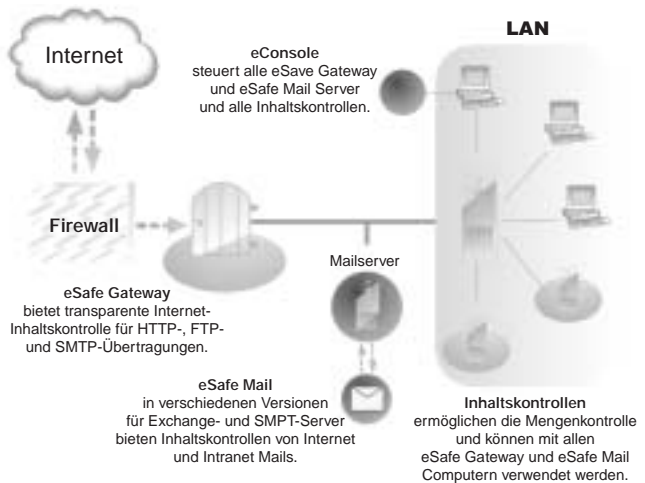
Um die Geschäfte zu betreiben, erlauben die Organisationen den Anwendern den Zugriff auf eine Vielzahl von Daten, von denen die meisten als vertraulich angesehen werden. Mit der Anwendung von Internet-Technologien, im Besonderen der eMail, sind diese Informationen nur einen Mausklick davon entfernt, an Unbefugte verschickt zu werden - egal, ob absichtlich oder unabsichtlich. Während Antivandalen und Antivirussoftware sowie Firewalls Hacker und feindliche Codes davon abhalten, diese Daten zu übermitteln, bieten sie keine angemessene Filterung der Inhalte von Sendungen. Ohne eine Filterung des eMail- und des anderen Internetverkehrs können Anwender einfach, gewollt oder ungewollt, vertrauliche Daten übermitteln. Das können z.B. vertrauliche Kundendaten, Passwörter, IT-Informationen, private Telefonnummern sein. Prozesse wegen sexueller Belästigung, Diskriminierung, Verstoß gegen Geheimhaltungsvereinbarungen und Fahrlässigkeit in Zusammenhang mit unangemessenem Gebrauch von eMail kosten die Firmen jährlich über 500 Mio. \$.

eSafe Gateway

eSafe arbeitet mit einer vorhandenen Firewall zusammen, um Viren und Vandalen auszuschließen.

Die revolutionäre Struktur von eSave Gateway vereint ein optimales Schutzniveau mit niedrigsten Verwaltungskosten. Dieses einzigartige Produkt ist aus vielen Gründen der "de-facto-Standard" für Gateway Inhaltssicherheit. Es ist für die Anwender transparent und erfordert weder die Installation von Software auf jedem einzelnen Arbeitsplatzcomputer noch Änderungen der Hardware.

eSafe Gateway ist ein leistungsstarker Antivandal- und Antivirus-Gateway der volle Inhaltssicherheit für jede innerhalb der Begrenzung des Netzes aufgenommene Verbindung bietet, einschließlich der Verbindungen durch jede Art von Firewall. eSafe Gateway war die erste inhaltsfilternde Software gegen Malicious Code und Viren für Firewalls. Daten, die über SMTP, HTTP und FTP Verbindungen laufen, werden gescannt und bereinigt. Sie kann entweder voll integriert mit einer Check Point Firewall-1 installiert werden oder als dual angelegtes Gateway in fast jeder Netzwerkumgebung.

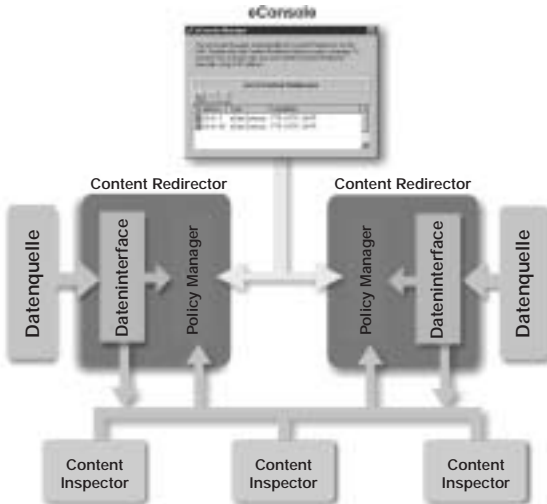


Nachdem eSafe Gateway in einer OPSEC-CVP Firewall-Umgebung (wie der Checkpoint Firewall-1) installiert ist, übergibt die Firewall jede infizierbare Datei (incl. Java-Applets und ActiveX-Objekte) für eine sofortige Prüfung an eSafe Gateway. Gleichzeitig werden alle nicht infizierbaren Dateien, wie Grafiken und reiner Text, ohne Verzögerung an die Empfänger weitergeleitet.

Wenn eine Firewall ohne CVP-Schnittstelle benutzt wird, arbeitet eSafe genau hinter der Firewall. Es empfängt den gesamten eingehenden Datenverkehr von der Firewall, scannt und routet den Verkehr entsprechend. Ausgehender Verkehr wird an eSafe Gateway geschickt, dann gescannt und weiter zur Firewall geleitet wird.

Die fortschrittliche modulare TECS Architektur

TECS™ steht für innovative, eSafe Total Enterprise Content Security Architektur. Diese Architektur ist sehr fortschrittlich, skalierbar, in Module aufgeteilt und verfügt über eine eingebaute Lastenverteilung.



Das TECS Architektur Diagramm

Die neuartige TECS Architektur besteht aus drei Hauptmodulen:

- **Content Redirector (CR)** - Der CR bestimmt, ob Inhalt zum CI (Content Inspector) weitergeleitet wird, und leitet geprüften Inhalt zu seinem vor gesehenen Ziel. Jeder CR kommuniziert entsprechend seiner bestimm ten Funktion mit einer spezifischen **Datenquelle**. Folgende Datenquellen stehen zur Verfügung:

- **Stand-alone Gateway** - benutzt NitroInspection für HTTP und FTP
- **CVP Firewalls** - OPSEC kompatible Firewalls
- **Microsoft Exchange Server -5.5 und 2000**
- **eSafe SMTP Mailprogramm** zusammen mit jedem SMTP Mailserver.

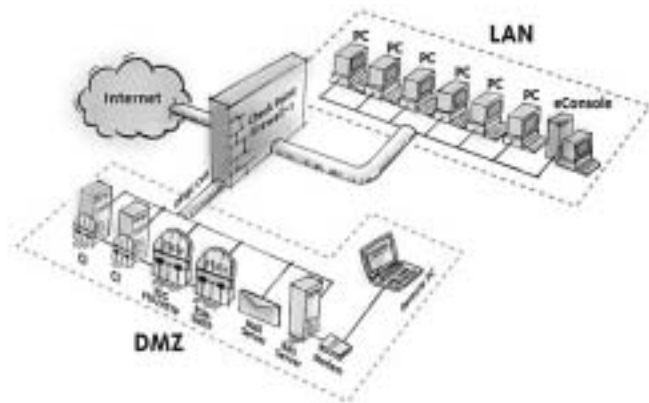
Der CR kommuniziert über die Content Inspector Remote (CIR) Komponente mit dem Content-Inspektoren.

- **Content Inspectors (CI)** - Entsprechend der Anforderungen können mehr als ein CI in der Infrastruktur installiert werden. Der CI scannt den Inhalt und erstattet dem CR Bericht, der dann den sicheren Inhalt an die Zieladresse weiterleitet. Malicious Code und anderer unerwünschter Inhalt werden blockiert und davon abgehalten, ihr vorgegebenes Ziel zu erreichen.
- **eConsole** - die eConsole konfiguriert und verwaltet alle eSafe Gateway und eSafe Mail Komponenten. Jeder CR enthält einen **Policy Manager**, der von der eConsole gesteuert wird.

Nahtlose Integration mit der FireWall-1

Über eine enge Abstimmung mit der Check Point FireWall-1 prüft eSafe Gateway den HTTP-, SMTP- und FTP-Datenverkehr und entfernt unerwünschte Inhalte. eSafe übernimmt das CVP-Konzept, das das System der Inhaltsprüfung vollständig in der DMZ anlegt und die Inhalts-Sicherheit in ein separates, sicheres Segment verlegt.

Einer der Hauptvorteile der OPSEC-CVP-Integrationen ist die Fähigkeit, spezielle Dateien mit schädlichem Inhalt zu behandeln, ohne dabei den Datenverkehr von Grafiken und Volltext zu beeinträchtigen. Zusätzlich erlaubt die intelligente CVP-Struktur eine vollständig plattformunabhängige Integration.



eSafe Gateway enthält die Möglichkeit einer sicheren, verschlüsselten Fernwartung, die von jedem Platz innerhalb der Organisation oder über das Internet gesteuert werden kann. eSafe erlaubt eine vollständige Skalierbarkeit und schließt die Unterstützung für das CVP Check-Point Load-Sharing mit ein. Entsprechend den Anforderungen können verschiedene eSafe Gateway-Produkte in einzelne Maschinen eingebaut werden, die dann zusammen in einem Load-Sharing-Cluster oder in einem protokollorientierten Inspektionsmodus für HTTP, SMTP oder FTP zusammenarbeiten.

Ein besonderes, einzigartiges Feature von eSafe für die FireWall-1 sind die zwei Methoden für die SMTP-eMail-Prüfung, die sich durch hervorragende Leistung und Stabilität auszeichnet.

Vorteile der OPSEC-Integration

- Es handelt sich um eine vollkommen modulare und skalierbare Lösung mit sicherer Fernwartung, unkomplizierter Installation und Integration in die Firewall.
- Isolierung des zu prüfenden Inhalts in der gesicherten DMZ.
- Die Isolierung von Inhalten, die geprüft werden müssen, verhindert eine Überlastung und Leistungsverluste.

Einsatz in jeder Netzwerkumgebung

Die besonders skalierbare und modulare aufgebaute NitroInspection-Architektur erlaubt die Installation von eSafe Gateway in Netzwerkumgebungen mit jeder Firewall. Die Vorteile liegen in der Unabhängigkeit vom CVP-Protokoll, da dieses Protokoll eine Reihe von Mängeln aufweist. Einer davon ist, dass derzeit nur die Check Point Fire Wall-1 mit dem CVP-Protokoll kompatibel ist. Ferner wirkt sich jedes CVP-Problem in der Firewall wiederum auf das gesamte Content Security Produkt aus. Wenn die Firewall im CVP-Modus arbeitet, muss der gesamte Datenverkehr zum Sicherheitssystem und wieder zurück geleitet werden, was bedeutet, dass dadurch der Datenfluss um einige Grade langsamer wird.

Durch die Unabhängigkeit von der Firewall ist mehr Flexibilität bei der integrierten Lösung für die Inhaltsprüfung möglich, was eine größere Geschwindigkeit und mehr Skalierbarkeit und Load-Sharing-Optionen erlaubt.

eSafe Gateway NitroInspection arbeitet wie ein doppelt angesteuertes Gateway zwischen Firewall/Router und LAN. Es kann auf zwei Arten installiert werden, entweder als Router oder im Brücken-Modus, die Installation erfolgt immer im Plug-and-Play-Verfahren.

Kein Verlust an Bandbreite

Die NitroInspection-Technologie erlaubt "on-the-fly" eine volle Prüfung unter dem Aspekt der Inhaltssicherheit aller per HTTP und FTP übermittelten Dateien, und zwar mit geringem Leistungsverlust im Netz.

Diese Methode, Dateien zu scannen, ist den älteren Proxymethoden, die von anderen Produkten eingesetzt werden, weit überlegen. Bei Proxymethoden ist erforderlich, dass das Tool für die Content Security die ganze Datei erhält und scannt oder genehmigt, bevor jegliche Übertragung zu den anfordernden Computern freigegeben wird. Das bedeutet Ausfallzeiten, Anwenderklagen wegen der langsameren Datenübermittlung im Netz und Probleme mit der Bandbreitennutzung. Die Proxymethode hat aber vor allem größere Einschränkungen.

Produkte für die Kontrolle von Inhalten, die die Proxymethode anwenden, fordern, dass alle Browser an Arbeitsplatzrechnern und alle andere Applikationen darauf programmiert werden müssen, mit dem Proxy zu arbeiten. Weitere Nachteile sind, dass diese Produkte den Protokoll-Durchgang auf vordefinierte Ports einschränken. Daneben geht einer der wichtigsten Vorteile von Proxyservern, nämlich das Caching, verloren, wenn in einem Unternehmen bereits ein anderer Proxy-Server installiert ist. Grund hierfür ist, dass das Content Security Produkt auf Proxy-Basis zwischen den Proxyservern und dem LAN installiert werden muss und somit in den gesamten Proxy-Verkehr eingreift, der dadurch mehrfach gescannt wird.

Unsere patentierte NitroInspection Technologie ist um ein Konzept herumgebaut, das den renommierten Untersuchungstechniken ähnlich ist, die von der Checkpoint Firewall-1 Produktlinie eingeführt wurden. Die Entwicklungsabsicht hinter NitroInspection war, eine Technologie zu entwickeln, die die Inhaltssicherheit des Proxymodells ohne die vorher erwähnten Nachteile bietet. Die NitroInspection Technologie sendet Datenpakete parallel und ermöglicht es auf diese Weise dem nachfragenden Computer und dem CI, die Datei gleich-

eSafeGateway kann in jede Netzwerkumgebung integriert werden - mit oder ohne Firewall

eSafe Gateway ist skalierbar und beeinträchtigt nicht die Performance der Firewall

eSafe Gateway benutzt die NitroInspection™ Technologie um sämtliche komprimierten und kodierten Dateien „on-the-fly“ zu untersuchen. Benutzerfreundlichkeit und Performance bleiben so erhalten

eSafe Gateway bietet verschiedene Skalierungsstufen und eine hohe Ausfallsicherheit dank Load-balancing und Fail-Over-Systemen

zeitig zu empfangen. So werden die Probleme der Proxymethode vermieden. Wenn das letzte Datenpaket den eSafe Gateway erreicht, wird es nur solange zurückgehalten, bis der CI die Untersuchung beendet hat. Sobald der CI die Datei gescannt und genehmigt hat, wird das letzte Paket an den nachfragenden Computer verschickt. Falls eine Datei eine Gefahr darstellt, verhindert eSafe Gateway die Weiterleitung des letzten Pakets an den nachfragenden Computer und erstellt eine oder mehrere vom Administrator konfigurierbare Nachrichten. Das erhält das hohe Sicherheitsniveau, das mit der Proxymethode verbunden wird.

Falls der Endanwender dennoch versucht, die Datei zu öffnen, dessen letztes Paket blockiert worden ist, informiert das Betriebssystem den Anwender, dass die Datei verfälscht wurde und nicht ausgeführt werden kann. Das verhindert, dass eine bösartige Datei den Endbenutzer gefährdet.

Zusammenfassend lässt sich sagen, dass es die revolutionäre Technologie, die durch NitroInspection verkörpert wird, eSafe ermöglicht, einen überlegenen Schutz - ohne oder nur mit geringem Einfluss auf den Datendurchsatz im Netz und die Erfahrung des Endbenutzers - anzubieten.

Load-Sharing-Fähigkeiten

Die wichtigste Leistungsanforderung im Umfeld der Content Security ist, aktuell ablaufende Prozesse auf schädliche Inhalte zu prüfen. Zunehmende Möglichkeiten und Fähigkeiten moderner Content Security Systeme erfordern insbesondere aber gerade im Zusammenhang mit der ständig anwachsenden Bandbreite fortschrittliche Loadsharing-Eigenschaften für mittelgroße und große Netzwerke. Die Prüfung des gesamten HTTP-Verkehrs, einschließlich der HTML-Seiten, ist sehr aufwändig. Gewöhnliche Antivirusprodukte haben deshalb diesen Datenverkehr bei Ihrer Überprüfung ausgespart. eSafe Gateway bietet flexible Lösungen, mit denen wirklich jeder Eingang behandelt werden kann, ohne dass die Sicherheit darunter leidet, weil die Prüfung von Webseiten unterlassen wird.

Das neue Architekturdesign von eSafe Gateway erlaubt die Konfiguration von mehreren CIs für den Einsatz in einer einzigen eSafe Gateway-Installation. Der CR kann die Inhaltsprüfung auf mehrere CIs verteilen.

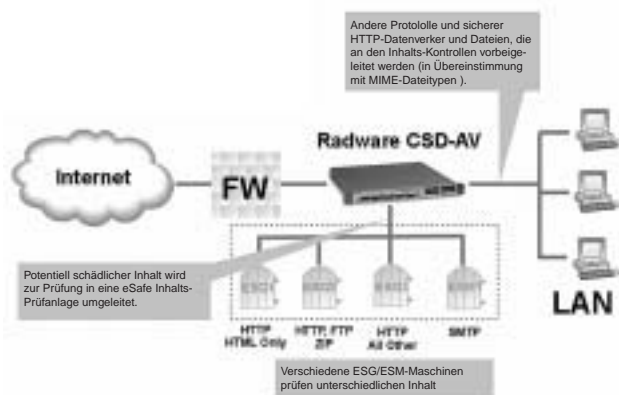
In größeren Netzwerken stehen bestimmte Ausgleichs- und Fehlerkorrektur-Lösungen bereit. eSafe Gateway kann in die Loadbalancing Soft- und Hardware von Drittanbietern integriert werden, wie zum Beispiel:

- Radware CSD-AV (siehe unten bzw. nächste Seite)
- StoneBeat SecurityCluster
- Alteon Web
- CISCO CSS
- F5 iTCM

Check Point FireWall-1 Netzwerke können eSafe Gateway im CVP Modus verwenden. eSafe Gateway unterstützt die Check Point CVP Eingangs-Balance-Architektur, die die Installation von mehr als eSafe Gateway als Sicherheits-Ressource ermöglicht.

Speziallösungen für Hochleistungs-Netzwerke

Für Netzwerke mit sehr hohen Datendurchgangskapazitäten haben Aladdin und Radware eine Spezialsoft- und Hardwarelösung entwickelt. Das Nitro-Inspection Routing (NIR) wird durch eine clevere Loadbalancing Vorrichtung ermöglicht. Das NIR-Design in eSafe Gateway basiert auf MIME Typen und stellt die einzigarte, zuverlässige Content Security-Lösung dar.



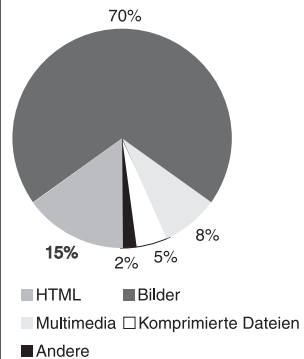
Die Radware CSD-AV ist eine intelligente ITM- (Internet Traffic Management) Einheit. Dabei werden fortschrittliche re-routing-Fähigkeiten eingesetzt. eSafe Gateway und seine Komponenten lassen sich nahtlos in diese Einheiten integrieren.

Dieses Hardware-beschleunigte intelligente Routing erlaubt eine um bis zu 500% schnellere Inhaltsprüfung und bietet fortschrittliche Skalierungsmöglichkeiten.

Nur 20% des Internet-Verkehrs wird als schädlich angesehen und der eSafe Gateway Bereich empfängt nur Inhalt, der potentiell gefährlich ist und gescannt werden sollte. Insbesondere größere Netzwerke profitieren von dieser Entwicklung, da Inhalte ohne Leistungsverlust vollständig überprüft werden können. So werden z.B. kritische und Realtime-Applikationen, wie Videokonferenzen, nicht durch die Inhaltsprüfung beeinträchtigt.

Die Aladdin-Radware-Lösung bietet weitere Vorteile, wie "Health-Monitoring", fortschrittliches Loadbalancing, Fehlerkorrektur und optional zusätzliche Sicherheitslösungen. Von Aladdin oder Radware kann auch ein separates Informationsblatt bezogen werden.

HTTP Traffic Analyse



Vollständiger Gateway-Virusschutz

eSafe Gateway benutzt eine moderne 32-bit-Scanning-Engine, um eine unbegrenzte Anzahl von Dateitypen zu scannen. Viele Virens Scanner, auch diejenigen, die in den eSafe-Produkten eingesetzt werden, sind von ICISA für die 100prozentige Identifizierung von Viren, die "im Umlauf" sind, zertifiziert. Trotzdem versagen die meisten, wenn es darum geht, Viren in komprimierten oder codierten Dateien aufzudecken. eSafe Gateway prüft und entdeckt auch alle Viren in .ZIP-, .ARJ-, .LHA-, .LZH-, .RAR-, .TAR-, .GZIP-, und .CAB-Dateien. Zusätzlich zu diesen Komprimierungsformaten kann eSafe Gateway Viren in MIME-, Uencode-, und BinHex-Anhängen entdecken.

eSafe Gateway benutzt dabei nicht die Dateieindungen, sondern analysiert mittels einer speziellen Vorgehensweise, die es nur bei eSafe gibt, die aktuelle Dateistruktur. Damit wird sichergestellt, dass Dateiverfälschungen ausgeschlossen sind. Zum Beispiel können Dateien verfälscht werden, indem die Dateieindung verändert wird oder mit anderen Methoden.

Außerdem verarbeitet eSafe Gateway Dateien, die mehrfach archiviert worden sind (zum Beispiel eine Zip-Datei in einer anderen Zip-Datei). Der Administrator kann die Zahl der Ebenen festlegen, in denen ein Archiv geöffnet und gescannt werden soll.

Die Macro Terminator™-Technologie macht es möglich, neue und unbekannte MS-Office-Makroviren durch den Vergleich bestimmter Muster, die von Makroviren benutzt werden, zu erkennen und zu entfernen. Lange Zeit wurden Makroviren als das größte Problem angesehen, aber die Makro Terminator™-Technologie beseitigt es auf beeindruckende Weise. Ein anderes einzigartiges System, die Ghost Machine™ Technologie, eliminiert neue polymorphe Viren, die ihren Code jedes Mal verändern, wenn sie eine Datei befallen. Dieses System führt solange Befehle in einer virtuellen, simulierten Umgebung aus, bis sich der Virus selbst entschlüsselt. Das steigert bedeutend die Fähigkeit von eSafe Gateway, neue polymorphe Viren schnell zu erkennen und mit ihnen umzugehen.

Mit der Makro Terminator Technologie erkennt und beseitigt eSafe Gateway über 90% der unbekanntesten Makro Viren.

Kompletter Schutz vor Vandalen

eSafe Gateway scannt den gesamten FTP-, SMTP-, und HTTP-Dateitransfer in Realtime nach Malicious Code in Java- und ActiveX Dateien. Alle Daten werden geprüft, noch bevor ihnen der Zutritt in das Netzwerk gestattet wird. eSafe Gateway schützt somit vor Malicious Code, der entwickelt wurde, um Daten zu zerstören oder zu stehlen und baut so eine sichere erste Verteidigungslinie für die Netzwerkressourcen auf.

eSafe Gateway schützt alle Ihre Daten, weil gefährlicher Java und Active X Code geblockt wird.

HTML-Vandals in Webseiten und eMails

Eine der wichtigsten Herausforderungen an eine moderne Content Security Lösung ist die Suche nach Malicious Code, wie z.B. nach schädlichen Skripten in HTML- oder XML-Inhalten. Mehr als 7% der Angriffe mit schädlichem Code erfolgten im Jahr 2001 mittels solcher Inhalte. Konventionelle Antivirus-Produkte bieten dafür keine Lösung - die Bedrohung durch solche Angriffe steigen aber stetig an. eSafe Gateway ist das erste Produkt, das solche Codes entfernen kann. Zusätzlich zu der Tatsache, dass es sich hierbei um das einzige Produkt handelt, das Signaturen von unbekanntem HTML/XML-Vandalen entdecken kann, verfügt eSafe auch über die fortschrittliche SmartScript™ Technologie. Diese entdeckt und blockiert proaktiv 98% der VBScript- und Javaskript-Vandalen, wenn sie zum ersten Mal auftreten. Diese Art von Malicious Code wird nicht immer von herkömmlichen Antivirus-Produkten er-

kannt. Dies liegt zum einen daran, dass der Code vollständig neu ist und dafür noch keine Signatur existiert, und zum anderen, weil HTML nicht vollständig gescannt wird. Die SmartScript Technologie wird eingesetzt, um Malicious Code zu blockieren, indem die schädlichen Aktivitäten analysiert und verhindert werden.

Das HTML/XML-Scanning kann individuell für HTTP und SMTP aktiviert werden. Wenn es in SMTP aktiviert wurde, bietet eSafe Gateway nicht nur Schutz vor angehängten Skript-Vandalen, sondern auch vor Malicious Code, der in eine HTML-formatierte eMail eingebettet ist, was die gängigste Art heutiger eMail-Anhänge darstellt. Der Administrator kann sogar die vollständige Eliminierung von eMail-Skripts einstellen, um somit jegliche Quelle für schädliche Aktivitäten auszuschalten.

Eine weitere Sicherheitsleistung, die in eSafe Gateway integriert ist, ermöglicht es, die Mehrzahl von Sicherheitslücken in der HTML-Syntax, in eMail-Überschriften und Inhaltsarten zu erkennen und zu schließen, wodurch verhindert wird, dass neuer Malicious Code durch diese Lücken eindringt.

Verhindern von Denial-of-Service-Angriffen

Zusätzlich zur Verhinderung von "unerlaubtem Zugang" für Malicious Code schließt eSafe Gateway ein weiteres kritisches Loch im Bereich der Content Security. Es werden Denial-of-Service-Angriffe blockiert, die in Form feindlicher Java und ActiveX Applikationen auftreten. Firewalls können viele Denial-of-Service-Angriffe eigenständig blockieren (wie das Überfluten oder Überlasten des Gateways durch Hacker, die damit erreichen, dass es nicht mehr funktioniert). Aber sie können nicht verhindern, dass Java-, ActiveX-Vandalen oder an E-Mails angehängte Programme damit beginnen, diese Angriffe direkt auf einer Workstation auszuführen. Das Problem ist, dass der Angriff erst gestartet wird, wenn das Java-Applet oder ActiveX-Control die Firewall passiert hat. Diese Angriffe schließen auch das Abschalten des Computers ein, wobei die gesamte, zur Verfügung stehende Speicherkapazität durch das Öffnen zahlreicher Fenster oder andere Vorgänge so stark beansprucht wird, bis das System zum Absturz gebracht wird. Einige neue DoS-Vandalen sind sehr gefährlich. Sie können einen gesteuerten DDos (Distributed Denial of Service)-Angriff auf wichtige Internetserver auslösen. Dabei werden Tausende infizierter Client Computer als Angriffsinstrument benutzt. Solche Attacken wurden 1999 eingesetzt, um große Websites wie Amazon.com, YAHOO.com und andere zum Absturz zu bringen. eSafe Gateway blockiert diese Art von Malicious Code in Java- und ActiveX, noch bevor sie in das Netzwerk gelangen - eine perfekte Ergänzung zum Schutz durch die Firewall.

Schutz vor der Enthüllung von Daten und vor Spam

eSafe Gateway kann einkommende oder abgehende eMails auf Grund von bestimmten Angaben wie z.B. Absender, Empfänger, Textinhalt oder Inhalt der Betreffszeile blockieren. Administratoren können bestimmte eMail-Mitteilungen mit verdächtigen Inhalten blockieren oder eine Kopie der Nachricht erhalten. So können eMails blockiert werden, die z.B. beleidigende Inhalte haben oder in denen vertrauliche Projektnamen auftauchen. Diese Funktion blockiert Mitteilungen, in denen gegen die Unternehmenspolitik verstoßen wird - und ermöglicht nebenbei eine unerwartete Stärkung dieser Politik. Auf diese Weise können auch Hacker- oder Vandalen-Angriffe abgewiesen werden, die SMTP benutzen, um gestohlene Informationen aus einem Netzwerk herauszuleiten. Zusätzlich hilft das Filtern der abgehenden eMails, die Sicherheit bezüglich der Unternehmensgeheimnisse, wie Passwörter und Informationen zu besonderen

eSafe Gateway kann Malicious Code aus eMails und Web Seiten entfernen.

eSafe Gateway stoppt die meisten Attacken, die durch eine Firewall alleine nicht verhindert werden können.

Projekten, zu stärken. Administratoren können veranlassen, dass eMails blockiert werden, die von eingetragenen Absendern eintreffen. Wird ein Malicious Code oder ein Virus in einer eMail-Mitteilung gefunden, kann die Adresse automatisch in die "Schwarze Liste" der Teilnehmer eingetragen werden. Das gibt dem Administrator die Möglichkeit, Spam zu blockieren ohne unbedingt die vollständige Adresse des Absenders kennen zu müssen und Absender zu blockieren, die möglicherweise Malicious Code oder Viren übermitteln. Das befreit Mailserver und Anwender von zeitraubenden Junk-eMails und potentiellen Virusinfektionen, ohne dass jede Mitteilung gescannt werden muss.

Andere Techniken, die dazu beitragen, Spam zu filtern, sind Schwarze Listen, die Hunderte von eMail-Parameter enthalten können, wie Überschriften, Text-Schlüsselwörter und Domains von bekannten Spammern.

Schutz vor Mail-Relaying, Spoofing und Bombing

eSafe Gateway stellt Einstellungsmöglichkeiten zum Schutz vor Mail-Relay zur Verfügung. Das verhindert, dass ungewollt eMail-Mitteilungen über den SMTP-Server umgeleitet und versendet werden. Auf diese Weise wird die Belastung reduziert und es wird verhindert, dass Spammer oder Hacker Ihren SMTP-Server für ihre Zwecke missbrauchen.

Der Schutz vor Spoofing stellt sicher, dass Außenstehende sich nicht als Personen ausgeben können, die zu Ihrer Organisation gehören, wenn sie eMails verschicken. Das schützt vor zwei beliebten Techniken - Fälschung und Personifizierung - die von Hackern und Computerkriminellen verwendet werden.

Der Schutz vor Mail-Bombing hilft bei schädlichen eMail DoS-Angriffen, die darauf abzielen, eMailserver zum Absturz zu bringen und Netzwerkverbindungen zu überlasten. Wenn ein eMail-Bombing-Angriff beginnt, wird er von eSafe Gateway entdeckt und blockiert.

Schutz durch automatische Lernprozesse

Wenn ein Malicious Code oder ein Virus entdeckt worden ist, kann eSafe Gateway automatisch zukünftige Downloads von dieser Site blockieren, indem die URL dieser Site in die "Schwarze Liste" eingetragen wird. Die gleiche Möglichkeit steht auch für eMails zu Verfügung. Der Administrator kann vorgeben, dass nur eine genaue Quelle (Datei, Seite oder Absender) oder der gesamte Server (oder eMail-Domain) blockiert wird. Außerdem können die Administratoren vorgeben, dass alle Dateien oder nur spezielle Dateitypen blockiert werden. So könnte ein Administrator zum Beispiel vorgeben, dass zukünftige Downloads von Grafiken und Texten gestattet werden, aber alle ausführbaren Dateien und Applets blockiert werden. Dadurch wächst die Effizienz enorm und es reduziert sich die Wahrscheinlichkeit des Eindringens von unbekanntem Viren in das Netzwerk.

Cookies, Skripts, Makros und Applet-Tags

Intelligentes Cookie Management - Diese Funktion ermöglicht den Administratoren die Kontrolle über Cookies. Diese kann so eingestellt werden, dass die Links zu allen Cookies getrennt werden, oder Links entsprechend verlässlicher und einschränkender Listen nur selektiv getrennt werden. Das sichert die vertraulichen Bereiche und verhindert, dass Hacker bereits bekannte Cookies dazu benutzen, an vertrauliche Daten zu gelangen. Gleichzeitig kann dieses Programm in bestimmten Sites, die für das tägliche Geschäft wichtig sind, die Verwendung von Cookies zulassen.

Neue Vandalen-/Virentabellen sowie neue Sicherheitskonfigurationen werden automatisch von der Aladdin FTP-Seite heruntergeladen.

Intelligente Skript-Filter - Diese Option ermöglicht den Administratoren, zu verhindern, dass bestimmte Skripte auf den Rechnern des Unternehmens ausgeführt werden. Unerwünschte oder gefährliche Arten von JavaScript-, VBScript-, oder JScript-Befehle können festgelegt und der HTTP-Datenverkehr bei Bedarf sofort gestoppt werden.

Ausschalten von Skripten

Diese Einstellmöglichkeit erlaubt es dem Administrator, jede Art von JavaScript, VBScript oder JScript aus Web Sites zu entfernen. Diese Option kann generell für alle Seiten eingestellt werden oder im Einzelfall für bestimmte Seiten, die entweder als vertrauenswürdig oder gefährlich eingestuft wurden. So kann ein umfassender Schutz vor Malicious Code, der in einer Skriptsprache erstellt wurde, sichergestellt werden.

Ausschalten von Java und ActiveX

Diese Option verhindert das Starten von Java Applets und Active X Controls und /oder das Ausführen von Befehlsparametern, die mit HTML Code den Browser zum Laden von Java oder ActiveX veranlassen. Leider kann hierdurch auch die Funktionalität einiger Websites eingeschränkt werden. Aus diesem Grunde ist der Einsatz dieser Funktion nur in Hochsicherheitsbereichen oder bei einem akuten Befehl von Malicious Code empfehlenswert

Entfernung von Makros

Makros werden in der Regel nicht zwingend benötigt und dienen meist zur Verbreitung von Makroviren, wie z.B. dem weitverbreiteten Concept Virus. Diese Funktion ermöglicht es dem Administrator sämtliche Makros aus MS-Office Dokumenten zu entfernen ohne dass dabei Texte oder andere Inhalte verändert werden. So lässt sich die Unternehmensrichtlinie, in der Makros grundsätzlich nicht erlaubt sind, durchsetzen. Daneben können auch unbekannte Makroviren erkannt und beseitigt werden - eine Funktion, die kein anderes Produkt bietet. Dies ist besonders bei "fremden" Dokumenten wichtig. So besteht die Möglichkeit sämtliche Makros aus Dokumenten zu entfernen, die nicht aus Ihrem Unternehmen stammen während die Makros in firmeninternen Dokumenten aktiv bleiben.

Entfernung von eingebundenen Objekten

Verschiedene Dateien lassen sich in MS Office Dokumente als Objekte einbetten. So z.B. Excel Tabellen in ein Word Dokument. Es können aber auch andere Dateitypen, die sich durch einen "Doppelklick" starten lassen (z.B. WAV Dateien), eingebunden werden. Daneben sind auch ausführbare Dateien und Skripte oder andere MS-Office Dokumente denkbar, die ebenfalls überprüft werden. Manche der eingebundenen Dateien/Skripte können gefährlich sein, die meisten sind jedoch unproduktiv oder nutzlos. Deshalb kann der Administrator diese Dateien aus den MS-Office Dokumenten entfernen. Potentielle Gefahren werden abgewehrt ohne den Inhalt der Datei zu beeinträchtigen. Diese Filterregel kann entweder nur auf alle Dateien unbekannter Herkunft oder auf alle User angewendet werden.

Sperren von unangemessenem Inhalt

Organisationen, die nach einem Internet-Inhaltsfilter suchen, haben folgende Ziele:

- eine Verbesserung der Mitarbeiterproduktivität
- erhöhte Sicherheit
- den Schutz der Netzwerk-Bandbreite
- eine Verringerung der juristischen Bedrohung

Optional kann ein URL basierter Filter von SurfControl mit derzeit 3.8 Millionen Webseiten und 42 Kategorien installiert werden.

Indem der Zugang zu manchen URLs oder Servern eingeschränkt wird, können Administratoren verhindern, dass Mitarbeiter auf Webseiten zugreifen, die im Widerspruch zur Unternehmenspolitik stehen. Webseiten können mittels einer Liste vordefinierter URLs oder IP-Adressen oder durch Wildcard-Zeichen definiert werden. Diese Liste kann schnell aktualisiert werden, wenn eine Webseite z.B. Hacker-Tools oder Trojanische Pferde enthält, die von eSafe Gateway entdeckt wurden. Weitere Downloads von dieser Webseite werden dann automatisch gesperrt, indem die URL, von der der Malicious Code oder der Virus geschickt wurde, automatisch in die Liste der zugangsbeschränkten Server eingetragen wird. Optional ist ein Plug-in (ab eSafe Gateway Version 3) erhältlich, das Webseiten mit unangemessenem Inhalt mittels einer vordefinierten und laufend aktualisierten Liste abgleicht und blockt. So können Sites in einer Liste spezieller URLs oder IP-Adressen oder über Wildcards definiert werden. Diese Liste kann auch jederzeit leicht aktualisiert werden. So kann eSafe Gateway zum Beispiel für die Zukunft Downloads von einer Site, auf der Hacker-Tools oder Trojanische Pferde entdeckt wurden, automatisch blockieren, indem die verdächtige URL in die "Schwarze Server-Liste" eingetragen wird.

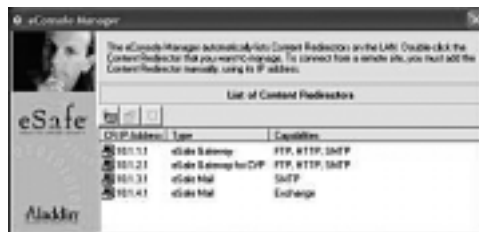
Eine neue Plug-In Option, die ab der eSafe Gateway-Version 3 zur Verfügung steht, enthält eine vorkonfigurierte und regelmäßig aktualisierte Liste mit Webseiten, die unzulässige Inhalte verbreiten. Mit derzeit über 3,8 Million URLs, die in 42 Kategorien aufgeteilt sind, gewährleistet diese URL-Liste, dass kein unzulässiger Inhalt in Ihr Netzwerk eindringen kann. Diese Datenbank ist von SurfControl®, lizenziert, einem der führenden Unternehmen, die URLs filtern. Diese Datenbank bietet den Unternehmen die Möglichkeit, Web-Inhalte einzuzugrenzen, ohne Arbeitskraft und Zeit auf die manuelle Pflege der "Schwarzen Listen" zu verschwenden. eSafe Gateway kann so konfiguriert werden, dass jede gewünschte Anzahl von Kategorien für jeden beliebigen Bereich blockiert werden (z.B.: Sport, Glücksspiel, Pornographie, Drogen, Gewalt, Rassismus, Reisen usw.). SurfControl erscheint bei Network Computing und IDC als "Nummer 1".

Sichere Fernsteuerung

Administratoren können eSafe Gateway und Mail von jedem Punkt im LAN oder über das Internet über eine sichere TCP/IP-Verbindung konfigurieren und steuern. Das erspart Administratoren, die nicht vor Ort sind eine Menge Zeit. Die gesamte Kommunikation zwischen eSafe Gateway, eSafe Mail und allen anderen Komponenten ist abgesichert.

Mehrfache Installationen und unterschiedliche Produkte können gleichzeitig über eine einzige eConsole verwaltet werden. So können XSPs mit Hilfe der Steuer-Console die Content Security der Produkte ihrer Kunden als Serviceleistung oder als Support anbieten. Große Organisationen können sie benutzen, um mehrfache Sites überall im Land und in der Welt zu steuern.

Sämtliche Einstellungen können remote über die eConsole vorgenommen werden.



Kundenorientierte Systemanforderungen

Die Möglichkeiten, die die fortschrittlichen Konfigurationsoptionen bieten, liegen in der automatisierten Säuberung, der Isolierung oder der Abweisung von infizierten oder feindlichen Dateien. Die unterschiedliche Vorgehensweisen werden dabei vom Administrator festgelegt. Der Schutz ist transparent und erfordert keinerlei Schulung. Infizierte Dateien können gereinigt, gelöscht oder isoliert werden. eSafe Gateway kann auch einen Warnhinweis in den eMail-Text einfügen. Administratoren können wählen, ob sie die Alarmmeldungen per Log-File, eMail, Netzwerk-Mitteilung oder als NT Event-Log empfangen wollen. Diese Meldungen können auch an Pager oder Mobiltelefone geschickt werden, die eMail-fähig sind. Die Administratoren definieren diese Methoden entsprechend der unten dargestellten Aufstellung.

eSafe Gateway verfügt über zahlreiche Reporting- und Benachrichtigungs-Tools



Zusätzlich können Administratoren eine eMail an den Absender der infizierten eMail schicken, in der mitgeteilt wird, dass seine Post blockiert wurde. Durch die Mitteilung an die Absender, dass eine Säuberung ihrer Systeme nötig ist, können zukünftige Probleme mit schädlichem Code und Kosten, die durch die Säuberung entstehen, vermieden werden. Wenn externe Absender benachrichtigt werden, dass ihr System eine Säuberung benötigt, hilft dies auch der Vorbeugung. Ohne diese Funktion könnte ein Kunde oder ein Lieferant weiterhin unbegrenzt Viren versenden.

Proaktives Aktualisieren

Das Proactive Update System, das in eSafe Gateway und eSafe Mail eingebaut ist, kann automatisch ein neues Update herunterladen (wenn nötig sogar stündlich) und kann jedes der folgenden Updates durchführen:

- Update der Signaturen für Malicious Code und Viren
- Aktualisierung der Schwarzen Liste für bekannte Vandalen
- Konfiguration der Produkt-Updates
- Aktualisierung der Datenbank der URL-Filter
- Upgrade der Product Engine

Neue Vandalen/Virus Listen werden genauso wie Security Updates automatisch von der Aladdin FTP Seite herunter geladen.

Dieses neue proaktive Update-System ermöglicht es ihrem CSRT nicht nur, Updates für Signatur-Tabellen zur Verfügung zu stellen, sondern auch sofort neue Updates für das Sicherheitssystem bereitzustellen (zum Beispiel die Blockierung von SHS-Dateien), wenn eine neue Gefahr erkannt wurde. Darüber hinaus kann im Zuge des Aktualisierungsprozesses eine interne eMail an den Administrator geschickt werden, in der ihm/ihr die neue Gefahr angekündigt wird und auch die Tatsache, dass sein/ihr System bereits davor geschützt wurde.

Anwenderrechte

In jeder Organisation gibt es bestimmte Personen, deren Aufgaben und Positionen es erforderlich machen, dass sie Zugang zu besonders vertraulichen Informationen haben. Für diese Bedürfnisse wird eine Liste privilegierter Anwender angelegt. Diesen Anwendern ist es erlaubt, Inhalte zu verschicken und zu empfangen, die normalerweise durch eSafe Gateway aufgehalten würden. In diese Liste können Arbeitsplätze, Server, Domains und E-Mail Adressen eingetragen werden.



eSafe Mail im Vergleich

Programmeigenschaft	eSafe Gateway	NAI WebShield	Trend Viruswall	Symantec WebSecure
Prüfung des HTTP, FTP und SMTP-Datenverkehrs	✓	✓ (3)	✓	HTTP, FTP
Skalierbare Architektur mit hoher Verfügbarkeit und Belastungsausgleich bei der Inhalts-Prüfung	✓	Nein	Nein	Nein
Fortschrittliche Methode, nicht auf Proxybasis	✓	Nein	Nein	Proxy
Kontrollpunkt CVP- (OPSEC) konform	✓	Nein	✓	Ohne OPSEC-Zertifikat
Filtert Java- und ActiveX-Vandale in HTTP	✓	✓	Nein (1)	Nein
Schützt vor bekannten und unbekanntem, schädlichen Skripten, die in Webseiten eingebettet sind	✓	Nein	Nein (1)	Nein
Filtert Java- und ActiveX-Vandale in eMails im HTTP-Format	✓	✓	✓	Nicht verfügbar
Schützt vor schädlichen VB/Java Scripten in eMails in HTML-Format	✓	Nein	Nein	Nicht Verfügbar
Heuristische Analyse - erkennt neue, unbekannte Macrovirten	✓	✓	✓	✓
Unterstützt Sicherheits-Einstellungen bei eMail-Anhängen	✓	✓	Nein (2)	Nicht verfügbar
Filter für eMail-Spam	✓	✓	Nein (2)	Nicht verfügbar
Kann jeder versendeten eMail Haftungsausschlüsse (Disclaimer) hinzufügen	✓	Nein	Nein (2)	Nicht verfügbar
Fügt automatisch belastigende Absender/Empfänger in Schwarze Listen ein	eMail / Sites / Domains	Nur Absender	Nein (2)	Nicht verfügbar
Sichere Fernverwaltung und Fernsteuerung auf TCP/IP-Basis	✓	✓	Nein (5)	Nicht verfügbar
Virens Scanner mit ICSSA- und Checkmark-Zertifikat	✓	✓	✓	✓
Kann Makros aus unsicheren Dokumenten entfernen	✓	Nur Filter	Nur Filter	Nein
Kann eingebettete Objekte aus OLE-Dokumenten entfernen	✓	Nein	Nur Filter	Nein
Proaktive Updates von Vandal/Virus-Tabellen, Schwarzen Listen, Konfigurations-Dateien und Sicherheitseinstellungen	✓	Nur DAT-Strukturen	Getrennte Updates für Maschine und Strukturen	Nur Virus-Strukturen
Zentrale Logdateien für Vorgänge in Mehrfach-Installationen	✓	✓	Nein (5)	✓
Entfernt bestimmte Arten von Anhängen (in Übereinstimmung mit Suffix oder Dateityp) Schließt Spoofing-Schutz ein	✓	✓ (4)	Nein (2)(4)	Nicht verfügbar
Optional Datenbank als URL-Filter	SurfControl 2.5 M 40 URL-Kategorien	Nein	WebMaster auf Proxy-Basis, Cyber Patrol mit 14 Kategorien	Im Leistungsumfang auf I-Gear-Basis-
Filter für HTTP auf Schlüsselwortbasis	✓	✓	✓	Nur HTTP
SMTP-Schlüsselwortfilter in: von/an/Betreff/Textfeld	✓	✓	Nein (2)	Nicht verfügbar
Anti-Relay und Anti-Bomb bei eMails	Y, Y	N, N	N, N	Nicht verfügbar

- (1) Zusatzmodul AppletTrap erforderlich, arbeitet als Proxy.
- (2) Zusatzmodul eManager erforderlich.
- (3) WebShield bearbeitet nur HTTP und FTP. WebShield SMTP bearbeitet SMTP. WebShield für Solaris bearbeitet alle drei Protokolle.
- (4) TVCS-Produkt erforderlich.

Eine vollständige oder teilweise Änderung der vorangegangenen Informationen bleibt vorbehalten. Aladdin Knowledge Systems, deren Tochtergesellschaften, Distributoren und verbundene Unternehmen übernehmen keine Haftung oder Verantwortung für die Vollständigkeit oder Genauigkeit der vorstehenden Informationen.

eSafe Mail

Eingebettete Skript-Vandalen sind für über 10 % der gefährlichsten Hacker- und Spionageangriffe verantwortlich.

eSafe Mail prüft den gesamten Internet- und Intranet E-Mailverkehr, der über SMTP-Mailserver oder Microsoft Exchange abgewickelt wird. Es schützt auch vor HTML-formatierten E-Mails. Diese E-Mails können aussehen wie ganz "normale Post", setzen aber den Anwender bestimmten gefährlichen Inhalten aus, wie z.B. feindliche Skripts, ActiveX, Java oder Plug-Ins.

Wenn eine infizierte E-Mail geöffnet wird, oder auch nur in einer Applikation in der Vorschau angesehen wird, können Vandalen aktiviert werden. Der Anwender merkt oft lange nichts davon, dass etwas falsch läuft, bis es dann zu spät ist. Und wenn das gesamte eMail-System infiziert ist, kann das verheerende Folgen haben.

eSafe Gateway prüft alle E-Mail-Sendungen einschließlich aller Arten von angehängten komprimierten Dateien (ZIP, TAR, LZH und andere), und zwar auch dann, wenn diese mehrmals komprimiert wurden. Außerdem werden alle MIME-Arten sowie die mit BINHEX und UUE verschlüsselten Dateien geprüft.

eSafe Mail vervollständigt eSafe Gateway bei der Bereitstellung eines vielschichtigen Schutzes. Die eingebauten Mail-Management-Funktionen machen die Verstärkung einer effizienten Sicherheitspolitik für alle in der Organisation im Umlauf befindlichen E-Mails möglich. Die Microsoft Exchange-Versionen arbeiten mit dem Mailserver zusammen und ergänzen seine Funktion, darin eingeschlossen das Scanning von Datenbanken.

Schutz vor Verbreitung sensibler Daten und Spam

Werkzeuge für die Prüfung von Inhalten steigern die Produktivität der Angestellten und reduzieren gleichzeitig die Belastung der firmeneigenen Bandbreite. eSafe Mail bietet eine Filterung auf der Grundlage von vorgegebenen Schlüsselwörtern, die auf unerlaubte Verbreitung von Daten oder unangemessene Inhalte schließen lassen. Spam-Filter reduzieren die Belastung durch eintreffende E-Mails, die den Benutzer Zeit kosten, anzügliche Inhalte besitzen und IT-Ressourcen verschwenden.

Skalierbare, Architektur mit hoher Verfügbarkeit

eSafe Mail ist in der Lage, große E-Mail-Aufkommen zu bewältigen. Wenn das Netzwerk und der Datenverkehr anwachsen, können Sie Content-Inspectoren hinzufügen, um die Belastung auszugleichen. Für eine noch größere Flexibilität können diese Content-Inspectoren mit eSafe Gateway geteilt werden. Die Architektur von eSafe Mail und eSafe Gateway bietet Ihnen die volle Kontrolle darüber, wie die Belastung verteilt wird. Es kann mehr als ein eSafe Mail pro SMTP installiert werden und damit auf der Grundlage von DNS eine hohe Verfügbarkeit erreicht werden. eSafe Mail für Exchange unterstützt die Version 5.5 und die Version 2000 und zieht Vorteile aus den Maschinen mit mehrfacher Integration (MS-VSAPI und MAP!). Außerdem werden Aktiv-Passiv- und Aktiv-Aktiv-Mailserver-Cluster unterstützt.

Flexible und mächtige Steuerung

Eine einfach zu benutzende Zentralkonsole ermöglicht es den Administratoren, die Content Security des Unternehmens im gesamten Netzwerk zu konfigurieren und zu verstärken. Die Steuerkonsole kann für alle eSafe Gateway- und eSafe Mail-Server verwendet werden, die in der Organisation installiert sind. Über diese Konsole kann die Konfiguration und Verwaltung ferngesteuert von jedem Ort im Unternehmen oder mittels Managed Service Providers (MSPs) über das Internet erfolgen.

Netzwerkadministratoren können individuelle Schutz-Levels festlegen und spezielle Regeln für spezielle Arbeitsplätze, Server, E-Mail-Adressen, E-Mail-Empfänger, Domains, Absender, Empfänger und Dateiartern definieren. Das ermächtigt die Feinabstimmung der Inhaltsprüfung und der E-Mail-Verwaltung.

Alarmmeldungen und Berichte

eSafe Mail erstellt für jedes Mal ausführliche Berichte, wenn ein Vandal in einer eMail-Sendung oder Datenbank gefunden wurde und alarmiert Sie. Die Berichte umfassen die Mailbox, Quelle und andere Kriterien.

Halten Sie Trojanische Pferde und Viren von Ihrem Netz fern

eSafe Mail sorgt dafür, dass keine Art von Malicious Code und Viren eindringen können. Beim Scanning entdeckt eSafe sowohl bekannte als auch unbekannte Trojanische Pferde, Würmer, Viren und Backdoors, indem ein Scanner benutzt wird, der sowohl von der ICSA als auch von Checkmark für das 100prozentige Aufdecken von im Umlauf befindlichen Viren zertifiziert ist.

Die Macro Terminator™ Technologie stoppt bekannte und unbekannte Microsoft Office Macroviern.

Die Ghost Machine™ stoppt polymorphe Viren und deren Mutationen, die Eintragungen in Skripte und die Tarntechniken gegen ihre Entdeckung anwenden.

eSafe Mail im Vergleich

Programmeigenschaft	eSafe Mail	McAfee WebShield	Trend ScanMail	Norton AV for Mail	Mail Sweeper
Unterstützt Microsoft Exchange und SMTP Mail Server	✓	✓	✓	Kein SMTP	✓
Filtert Java- und ActiveX Vandalen in eMails im HTML-Format	✓	✓	Nein	Nein	Nein
Schützt vor bekannten und unbekanntem schädlichen Skripten in eMails im HTML-Format	✓	Nein	Nein	Nein	Begrenzt
Heuristische Analyse - erkennt neue, unbekannte Makroviren	✓	✓	✓	✓	Nicht verfügbar, externes Programm erforderlich
Schlüsselwörterfilter in: von/an/Betreff/Textfeld	✓	✓	Nein (1)	Nein	✓
Unterstützt Sicherheitseinstellungen bei eMail-Anhängen	✓	✓	Nein (1)	✓	✓
eMail-Spam-Filter	✓	✓	Nein (1)	Nein	✓
Kann jeder versendeten eMail Haftungsausschlüsse (Disclaimer) hinzufügen	✓	Nein	Nein (1)	Nein	✓
Fügt automatisch belastigende Absender/Empfänger in Schwarze Listen ein	✓	Nein	Nein	Nein	Nein
Sichere Fernverwaltung und Fernsteuerung auf TCP/IP-Basis	✓	✓	✓	✓	Nicht verfügbar Programm nicht im Lieferumfang
Kann Makros aus unsicheren Dokumenten entfernen	✓	Nur Filter	Nur Filter	Nein	Nein (2)
Kann eingebettete Objekte aus OLE-Dokumenten entfernen	✓	Nein	Nur Filter	Nein	✓ (3)
Fügt automatisch belastigende Absender/Empfänger in Schwarze Listen ein	eMail / Site / Domain	Nur Absender	Nein (1)	Nur Absender	Nein
Proaktive Updates von Vandal/Virus-Tabellen, Schwarzen Listen, Konfigurations-Dateien und Sicherheitseinstellungen	✓	Nur DAT-Strukturen	Getrennte Updates für Maschine u. Strukturen	Nur Virus-Strukturen	Nicht verfügbar - Programm nicht im Lieferumfang
Zentrale Logdateien für Vorgänge in Mehrfach Installationen	✓	✓	TVCS erforderlich	Nein	Nein
Skalierbare Architektur mit hoher Verfügbarkeit und Belastungsausgleich bei der Inhaltsprüfung	✓	Nein	Nein	Nein	Nein
Entfernt bestimmte Arten von Anhängen (in Übereinstimmung mit Suffix oder Dateityp) Schließt Spoofing-Schutz ein	✓	Kein Anti-Spoofing für Dateien	Kein Anti-Spoofing für Dateien	Kein Anti-Spoofing für Dateien	Kein Anti-Spoofing für Dateien

Spezielle Eigenschaften für Microsoft Exchange

Unterstützt Exchange APIs (5)	MAPI und AVAPI	AVAPI	AVAPI oder ESEAPI (5)	AVAPI	AVAPI
Unterstützt Exchange Cluster	✓	✓	✓	✓	✓

- (1) eManager erforderlich.
- (2) Zusatz. Eingeschränkt. Langsam. MS Office 2000 muss auf dem selben PC installiert sein. Kann nicht nur unsichere Quellen filtern.
- (3) Kann nur alle filtern. Kein Scanning oder Filtern von sicheren Quellen.
- (4) Die Version 1.0 der Microsoft Antivirus Programm-Schnittstelle wurde AVAPI genannt. Die Versio 2.0 (liegt in Exchange 2000 vor) wird VSAPI genannt (Virus Scn API).
- (5) Die Microsoft Extensible Storing Engine (ESE) API ist für Backup-Applikationen gedacht und wird von Microsoft nicht als ein Antivirus API unterstützt oder eingefügt.

Eine vollständige oder teilweise Änderung der vorangegangenen Informationen bleibt vorbehalten. Aladdin Knowledge Systems, deren Tochtergesellschaften, Distributoren und verbundene Unternehmen übernehmen keine Haftung oder Verantwortung für die Vollständigkeit oder Genauigkeit der vorstehenden Informationen.

Die eSafe Appliance

Die eSafe-Appliance ist das erste Check Point OPSEC kompatible Produkt für Inhaltssicherheit und Virenbekämpfung für den industriellen Einsatz.

Sie arbeitet als dedizierter Server, ist mit einem gehärteten Betriebssystem ausgestattet und wird mit der preisgekrönten Software eSafe Gateway und/oder Mail ausgeliefert.

Sie kann einfach in jede bestehende Sicherheitsinfrastruktur eingebaut werden und jederzeit zu einer hochwertigen, kostengünstigen Content Security Lösung ausgebaut werden.



Die eSafe Appliance wird vorinstalliert und vorkonfiguriert verschickt, um Kosten zu sparen, die bei der Hardware-Beschaffung, der Lizenzierung der Betriebssoftware und bei der Softwareintegration entstehen. Ebenso wichtig ist, dass die Administratoren sich nicht um komplizierte und zeitraubende Installation und Integration von verschiedenen Antivirus- und Content-Sicherheits-Produkten von verschiedenen Herstellern kümmern müssen.



Die Anwendersoftware selbst entspricht höchstens Qualitätsanforderungen und ist für eine zuverlässige und leistungsfähige Integration auf Komponentenbasis geeignet. Sie ist für mittlere bis mittelgroße Unternehmen geeignet, die nach einer proaktiven Lösung für die Sicherheit von Internetinhalten suchen, die leicht zu installieren und zu pflegen ist.

Vorteile im Einzelnen

- Hohes Sicherheitsniveau mittels eines gehärteten Betriebssystems
- Hohe Systemleistung durch eine straffere Hardwareintegration und -optimierung
- Hohe Verfügbarkeit durch eingebauten Lastenausgleich
- Einfache GUI-Steuerung
- Einfache Verwaltung und Kontrolle direkt vom Desktop durch optimierte Protokolle und Statistiken
- Einfaches updaten der Virustabellen, Content Security Engine, Listen, Konfigurationsdaten sowie des entsprechenden eSafe Produkts
- Der ROI ist wegen der reduzierten Integrationskosten und einer schnelleren Entwicklung besser
- Out-of-the-box Content Security Lösung mit einer hervorragenden Voreinstellung, die im Bedarfsfall jederzeit angepasst werden

Kompatibilität & Verfügbarkeit

eSafe Gateway steht in unterschiedlichen Versionen zu Verfügung, um den verschiedenen Anforderungen des Unternehmens gerecht zu werden. Prüfen Sie deshalb ihre Anforderungen, bevor Sie eine Testversion oder eine Lizenz anfordern. Die Stand-Alone-Version kann nur in einigen Umgebungen installiert werden und hängt von der Art der Firewall ab. Diese Version kann in Netzwerken mit oder ohne Firewall eingesetzt werden.

eSafe Gateway und eSafe Anwendungen sind auch vollkommen OPSEC-kompatibel, was bedeutet, dass sie mit Firewalls arbeiten können, die mit dem CVP-Protokoll von Check Point kompatibel sind.

eSafe Gateway kann auf jedem PC installiert werden, der die Mindestanforderungen bezüglich der Hardware erfüllt. Es gibt Versionen für Windows und Linux.

eSafe Mail ist für Microsoft Exchange 5.5 und 2000 und für SMTP Mail-Server erhältlich. eSafe Mail kann in jedem PC installiert werden, der die Mindestanforderungen bezüglich der Hardware erfüllt. Es stehen Versionen für Windows NT/2000/XP und Linux zur Verfügung.

Preise und Auszeichnungen



eSafe Mail
July - 2001



eSafe Gateway
July - 2001



eSafe Mail for
Exchange
July - 2001



eSafe Appliance
July 2000

Über Aladdin...

"Gateway-to-Desktop"-Schutz für Unternehmen bereit. Die nächste Generation bei der Hardware-Authentisierung ist **eToken®**, es handelt sich dabei um einen USB-Token für eine sichere Speicherung von Zertifikaten und Anwender-Daten. Die Liste schließt auch **HASP®** und **Hardlock®** ein, zwei hardware-basierte Software-Schutzsysteme, die Lizenzschutz gewährleisten, eine innovative Lizenzvergabe, Test- und Upgradelösungen für Softwareentwickler und -herausgeber unterstützen. Bei **Privilege®** handelt es sich um eine Serie von Software-Lizensierungs- und Vertreibertools, die im Internet bereitgestellt werden. Aladdin unterstützt Software- und Internet-Sicherheitslösungen weltweit bei Millionen Personen und Gesellschaften, einschließlich der wichtigsten Banken, Finanzierungsinstitute, Fortune 100-Gesellschaften, der Bundesregierung, Universitäten und die wichtigsten Bildungsinstitute. Der Hauptsitz des Unternehmens liegt in Tel Aviv, Israel. Für weitere Informationen besuchen Sie bitte die Aladdin-Homepage unter <http://www.Aladdin.de> oder die Homepage für die Sicherheitsabteilung von Unternehmen unter: <http://www.eSafe.com>.



Weitere Informationen finden Sie unter: www.Aladdin.de

Germany

T: +49-89-89-4221-0, F: +49-89-89-4221-40, info.esafe@Aladdin.de
Gabriele-Münter-Str. 1, D-82110 Germering

