Alles in einem und virtuell

Anti-Malware- und Performance-Qualität virtueller UTM-Appliances

Virtuell ist „in" – teils auch schon bei Sicherheitssystemen. Die <kes> wollte daher wissen, wie es um den Malware-Schutz und die Performance von virtualisierten UTM-Appliances steht. Sechs Systeme haben sich unseren Testern gestellt.

Von Bernhard Stütz und Thomas Rottenau, Stralsund, sowie Guido Habicht und Maik Morgenstern, Magdeburg

Im Zeitalter von Unified-Communications müssen Security-Appliances die Sicherheit unterschiedlichster Dienste sicherstellen. Neben den dienstleistenden Servern migrieren zunehmend auch die Schutzsysteme in virtualisierte Umgebungen. Einige Hersteller bieten deshalb ihre Security-Appliances auch bereits als virtuelle Maschinen an oder ihre Sicherheitslösung lässt sich zumindest in einer virtuellen Umgebung installieren. Neben einer leichteren Skalierbarkeit versprechen derart virtualisierte Schutzverfahren nicht zuletzt auch geringere Kosten.

Neben dem monetären Aufwand für Anschaffung und Wartung haben Sicherheitslösungen aber auch ihren Preis in der „Währung Performance": Das Verhalten vieler Dienste ist sehr von der Verzögerungszeit (Latenz) auf den Netzwerkverbindungen abhängig. Sicherheitslösungen bewirken häufig eine nicht unerhebliche Latenzzeit und damit oft verbunden einen hohen „Jitter" für die Daten, sprich es kommt zu Schwankungen im Datendurchsatz. Generell kann eine Security-Appliance den Durchsatz oft unerwartet stark begrenzen: Gerade wo alle Algorithmen in Software ablaufen, unterscheidet sich das zeitliche Verhalten deutlich von hardwarebasierten Komponenten wie Switches und Routern.

Da sich derartige Tests in Produktivumgebungen naheliegenderweise verbieten, haben die Autoren für die <kes> im Labor die Performance und den Malware-Schutzlevel der im „virtuellen UTM"-Segment erhältlichen Produkte ermittelt (s. a. Hinweis im Kasten „Produkte im Test").

Produkte im Test

Astaro Security Gateway (Version 7.501)
Collax Security Gateway (Version 5.0.6)
Endian Firewall Software Appliance (Version 2.3-0)
Gateprotect (Version 8.5)
Kerio Winroute Firewall (Version 6.7.1 build 6399)
XnetSolutions SXGate (Version 5.1-1-2)

Die ursprünglich ebenfalls zum Test vorgesehene Securepoint UTM Security (Version 10) konnte aufgrund von Supportengpässen beim Anbieter während des Testzeitraums leider nicht evaluiert werden. Durch personelle Veränderungen in einem der beteiligten Häuser musste zudem die abschließende Auswertung und Veröffentlichung der Testergebnisse deutlich verschoben werden. Während die Autoren in der Vorbereitungsphase bemüht waren, mit dem Testfeld eine möglichst vollständige Marktabdeckung zu erreichen, können daher zum Zeitpunkt des Erscheinens dieses Berichts durchaus zusätzliche Angebote auf dem Markt virtualisierter UTM-Appliances existieren.

Testverfahren

Alle Produkte wurden auf derselben Hardware- und Virtualisierungsplattform installiert, um eine Vergleichbarkeit der Performanceergebnisse zu gewährleisten. Die AV-Test GmbH testete den Schutzlevel der Appliances in Sachen Malware, während das „Steinbeis Transferzentrum Projektierung und Evaluierung von Netzwerken" an der Fachhochschule Stralsund die Performance der Produkte untersuchte (s. a. Kasten auf S. 32).

Die getesteten Security-Appliances liefen als einzige virtuelle Maschine auf einem leistungsfähigen Server mit VMware. Die virtuellen Netzwerkinterfaces wurden auf drei physische Gigabit-Ethernet-Netzwerkkarten abgebildet, die mit drei verschiedenen Netzen – einem „externen", internen und Management-Netz – verbunden waren. Der verwendete Server zur Bereitstellung von Malware-Samples und „sauberen" Inhalten (zur Erkennung von Fehlalarmen) sowie die Testclients wurden auf einem zweiten virtualisierten Server ausgeführt, der mit derselben Netzstruktur verbunden war (vgl. Abb. 1). Für die Systeme

auf diesem zweiten Server kam virtualisiertes Windows XP zum Einsatz.

Malwaretests

Um einen vorbereiteten Malware-Test zu starten, verbindet sich der Client mit dem Malware-Server und teilt ihm mit, welcher Test durchgeführt werden soll. Während des Tests ruft der Client dann eine Liste von Dateien ab und analysiert nach Abschluss aller Transfers die übertragenen Daten – dabei legt das System detaillierte Log-Dateien an, die MD5-Kontrollsummen und HTTP-Response-Codes enthalten. Alle übermittelten Inhalte werden zudem für weitere Analysen in ZIP-Archiven auf dem Client gespeichert.

Nach den Testläufen vergleichen die Tester die MD5-Hashes der ursprünglichen Dateien des Malware-Servers mit den MD5-Werten auf dem Client: Sind sie identisch, wurde der Inhalt eins zu eins übertragen – weichen sie voneinander ab, die Daten wurden aber übermittelt, so hat die Appliance die Datei offensichtlich modifiziert. Eine vollständig transferierte Datei wird abhängig vom Testfall als negativ bewertet, wenn es sich um Malware handelt, oder als positiv, sofern es eine „saubere“ Datei in einem Fehlalarm-Testszenarium war.

Liegen auf dem Client keine Daten zur Berechnung einer MD5 Kontrollsumme vor, wird die entsprechende Datei als „blockiert“ gewertet, also positiv in einem Test auf Malware oder negativ beim Fehlalarm-Test. Einige Appliances präsentieren dem Nutzer eine „Block-Seite“ anstatt den Inhalt der Datei zu übertragen: Der Inhalt solcher Seiten wurde ebenfalls gespeichert und entsprechend bewertet. Im Fall von nur teilweise übermittelten Daten wurden zusätzliche Kontrollen durchgeführt.

Zur Charakterisierung des Schutzgrades einer Security-Appliance gegen Malware eignet sich neben der **Erkennungsrate** bekannter Viren, Würmer und Trojaner auch die **Häufigkeit von Fehlalarmen**, also der Anteil „sauberer“ Dateien, die fälschlicherweise als Malware erkannt werden. Neben einer direkten Übermittlung wurden die Samples zudem in verschiedenen **Archiv-Formaten** verpackt transportiert. Die Dateibasis auf dem Malware-Server bestand für den Test aus 3929 infizierten Dateien aus der „WildList“ – einer Sammlung von zum Testzeitpunkt weit verbreiteter Schadsoftware – und zusätzlich aus 400 nicht-infizierten Dateien zur Prüfung auf „False Positives“. Diese Daten wurden sowohl über HTTP als auch über das POP3-Protokoll durch die Appliance übertragen, wobei jeweils Erkennungs- und Fehlalarmrate bestimmt wurden. Diese Messungen wurden zunächst ohne Zusatzlast auf dem Netzwerk durchgeführt (siehe aber auch „Kombinierte Tests“).

Performancetests

Zur Performancemessung kamen zusätzlich am „externen“ Switch ein Smartbits Lastgenerator- und Analysator (Serverport) sowie ein Applikationssimulationsserver Spirent Reflector zum Einsatz. Im internen Netzwerksegment arbeiteten der Clientport des Smartbits und der Clientsimulationsserver Spirent Avalange. Der Lastgenerator/Analysator Smartbits 6000C diente den UDP-Durchsatzmessungen, die Avalange/Reflector-Kombination für TCP- und HTTP-Messungen.

Die Servertestports können übliche Netzwerkdienste mit hoher Performance (Linespeed 1 Gbit/s) bereitstellen, die Clienttestports der Systeme viele gleichzeitige Verbindungen durch die Appliance hindurch zu den Servertestports aufbauen. Beide Seiten lassen sich für unterschiedliche IP-Protokolle, Rahmenlängen (Frame Size) und -raten sowie die Anzahl der gleichzeitigen Verbindungen konfigurieren. Die Generatoren erzeugen und senden dabei die gewünschten Frames, die Analysatoren empfangen und verarbeiten die übermittelten Daten.

Bei der durchgeführten **UDP-Durchsatzmessung** handelt es sich um eine standardisierte (RFC 2544) Baselinemessung, welche den Netzwerk-Durchsatz ohne Protokolleinflüsse der Appliance (wie sie bei TCP unvermeidlich sind) und bei unterschiedlichen Rahmenlängen

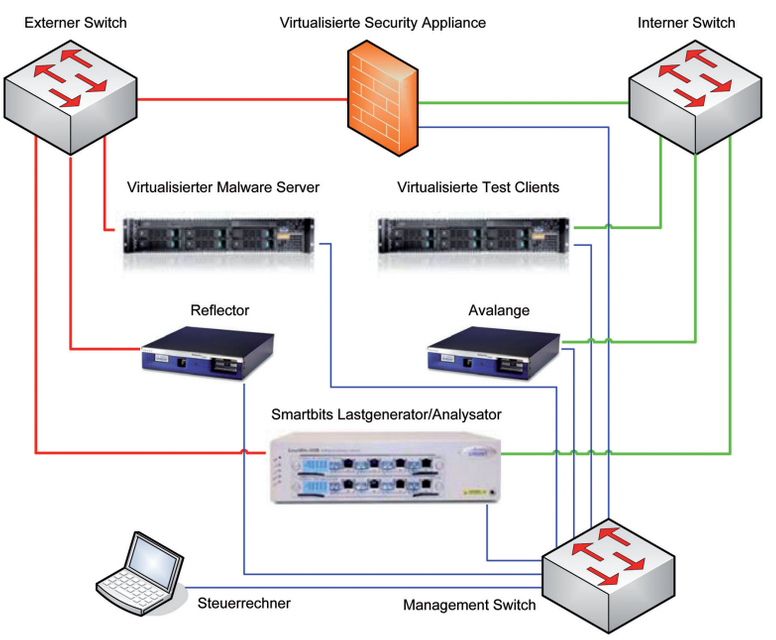

Abbildung 1: Testaufbau

bestimmt. Obwohl diese Messungen nicht sehr realitätsnah sind, werden sie als Vergleichsmaßstab geschätzt, da sie sehr gut zu reproduzieren sind. Von sieben im Standard definierten Framegrößen wurden im Test fünf genutzt: 64, 256, 512, 1024 und 1518 Bytes. Die kurzen Rahmenlängen stellen dabei die höchste Belastung für eine Appliance dar, weil dabei die größte Anzahl von Rahmen/Sekunde bei ansonsten gleicher Datenrate (Bytes/Sekunde) verarbeitet werden muss. In der Praxis sind ungefähr die Hälfte aller Rahmen 64 Byte lang, da in solchen kurzen Frames die TCP-Acknowledge-Pakete übertragen werden.

Pro Rahmenlänge wird im Test die Last stufenweise erhöht, bis Rahmenverluste auftreten – der UDP-Durchsatz wird als diejenige Last festgelegt, die gerade noch ohne Rahmenverluste funktioniert hat. Außer der isolierten Bestimmung des UDP-Durchsatzes für die fünf verschiedenen Rahmengrößen, haben die Tester noch eine Messung des UDP-Durchsatzes mit einer realitätsnahen Mischung unterschiedlicher Rahmengrößen durchgeführt: Diese „IMIX"-Messungen (Internet-Mix) sind nicht standardisiert; als Grundlage diente eine statistische Erfassung des MCI-Backbones.

Näher an der Realität ist auch die Bestimmung der **TCP-Übertragungsleistung:** TCP-Verkehr wird in einer Security-Appliance mittels Stateful Inspection überwacht, die Übertragungsleistung hängt von Parametern wie Netzwerkverzögerung, Anzahl gleichzeitiger Verbindungen und der Datenmenge pro Verbindung ab. Beim Testverkehr wurden pro TCP-Verbindung 10 Übertragungen mit je 10 kByte Nutzdaten gestartet. Die ermittelte TCP-Übertragungsleistung ergibt sich als erfolgreich durchgeführte Nutzdatenübertragung (in MBit/s) gemittelt über den Testzeitraum von 100 Sekunden.

Da eine Stateful-Inspection-Firewall für jede TCP-Verbindung einen Eintrag in einer Verbindungs-Tabelle zur Überwachung benötigt, verbrauchen TCP-Verbindungen durch eine Firewall Hauptspeicherplatz. Der Speicherbereich wird auch nach Beendigung der Verbindung noch so lange belegt, bis die „Time-Wait"-Zeit (bis zu 4 Min.) der TCP-Verbindung abgelaufen ist. Bei vielen kurzen Verbindungen (ein recht häufig auftretender Effekt, wenn beispielsweise viele Menschen gleichzeitig im WWW surfen) kann diese Tabelle überlaufen, was je nach Firewall-Implementierung unterschiedliche Effekte bewirkt. Zur Bestimmung der Anzahl **gleichzeitig möglicher TCP-Verbindungen** wurden pro Sekunde 1000 neue Verbindungen aufgebaut, über die Messzeit offen gehalten und mit einem Request (Transaktion) getestet – pro Messzyklus von 100 Sekunden können mit dieser Konfiguration also maximal 100 000 TCP-Verbindungen aufgebaut werden. Vor dem Verbindungsabbau wurde mit einer weiteren Transaktion pro Verbindung getestet, ob diese noch verfügbar ist. Die erste nicht-erfolgreiche Transaktion markierte dann die maximale Anzahl gleichzeitiger TCP-Verbindungen durch die Security-Appliance.

Abbildung 2: Die Langzeitmessungen mit und ohne Malwarelast zeigten bei der Astaro-Appliance nur vereinzelte Einbrüche der Übertragungsrate – allerdings mit vergleichsweise niedrigem Durchsatz.

Bei der Messung der **HTTP-Übertragungsleistung** wurde überprüft, wie sich die Analyse des übertragenen Inhalts bei HTTP-Verbindungen auf die Übertragungsleistung auswirkt: Der HTTP-Verkehr wird auf der Security-Appliance über ein transparentes Proxy geleitet, das den Datenverkehr auf Malware untersucht und infizierte Dateien blockiert oder modifiziert. Die Übertragungsleistung wird in diesem Fall von vielen Parametern beeinflusst: Der Inhalt hat einen großen Einfluss, zum Beispiel müssen Archive vor der Prüfung zuerst ausgepackt werden. Diese Proxy-Aktivitäten führen zu einer Verzögerung, welche wiederum die Übertragungsleistung beeinflusst. Pro HTTP-Verbindung wurden 10 Übertragungen mit je 10 kByte Daten initiiert. Die HTTP-Übertragungsleistung ergibt sich aus der Anzahl der durchgeführten GET-Requests multipliziert mit der Nutzdatenlänge und gemittelt über die Messzeit in der Maßeinheit MBit/s.

Zudem wurde analog zu TCP die **Anzahl gleichzeitig möglicher HTTP-Verbindungen** ermittelt. Da ein Proxy die Verbindungen zum Client terminiert und zum Server eine weitere Verbindung aufbaut, verdoppelt sich bei HTTP-Traffic die Anzahl der Verbindungen durch die Security-Appliance. Diese Anzahl kann weiter ansteigen, wenn HTTP 1.0 zum Einsatz kommt, wo für jeden GET-Request eine eigene Verbindung aufgebaut wird. Zur Bestimmung dieser Kenngröße wurden pro Sekunde 1000 neue HTTP-Verbindungen aufgebaut – mit einem GET-Request pro Messzeit und offen bleibender Verbindung. Pro Messzyklus von 100 Sekunden ließen sich somit maximal 100 000 HTTP-Verbindungen aufbauen – die erste nicht-erfolgreiche Transaktion markierte die maximale Anzahl gleichzeitiger HTTP-Verbindungen über das Proxy der Security-Appliance.

Kombinierte Tests

Um eine eventuelle Reduzierung der Malware-Testtiefe bei hohen Lasten ausschließen zu können,

wurde die **Anti-Viren-(AV)-Erkennungsrate unter hoher Netzwerklast** geprüft, indem die Wildlist-Malware-Erkennungsrate unter maximaler HTTP-Netzwerklast wiederholt wurde.

Die HTTP-Übertragungsleistung wurde über die Kurzzeittests hinaus auch für den Zeitraum einer ganzen Stunde durchgeführt, um das **Langzeitverhalten** der Appliances zu dokumentieren. In einer zweiten Langzeitmessung wurde zudem die **HTTP Übertragungsleistung mit Malwarelast** ermittelt, um das Langzeitverhalten der Appliances „unter Beschuss" zu dokumentieren – die Ergebnisse dieser Messung sind in den abgebildeten Grafiken zu jeder Appliance wiedergegeben.

Ergebnisse

Alle numerischen Messwerte finden Sie zusammen mit der Featureliste der getesteten Systeme in der umfassenden Tabelle auf Seite 32. Im Folgenden sind zudem Besonderheiten und kurze Zusammenfassungen der Testergebnisse aufgeführt. Weitere detaillierte Messergebnisse und Grafiken sind bei Interesse über www.stz-netze.de/kes-test abrufbar.

Astaro Security Gateway

Das Astaro Security Gateway (Version 7.501) lässt sich vollständig und umfassend über ein Webinterface (GUI) einrichten. Allerdings stellt es – außer nach dem allerersten Login – keine „Wizards" zur Verfügung, sodass die Konfiguration teilweise etwas umständlich ist. Im Test fiel zudem auf, dass die POP3-Quarantäne die Festplatte vollschreiben kann: Sobald kein Festplattenplatz mehr verfügbar ist, können über das System jedoch keine weiteren Verbindungen aufgebaut werden – die Appliance schottet sich quasi komplett nach außen hin ab, es kann dann zwar keine Malware passieren, aber auch „sauberer" Datenverkehr gelangt nicht mehr durch das Gateway hindurch. Das Löschen des POP3-Caches war außerdem nicht über das GUI möglich: Trotz eines entsprechenden Dialogs wurden die E-Mails nicht entfernt. Über die Konsole war eine Löschung hingegen erfolgreich, sodass anschließend der normale Betrieb weitergehen konnte. Für die nächste Version hat Astaro einen Fix angekündigt.

Die Malware-Erkennung erreichte sowohl bei HTTP als auch bei POP3 100 %, auch unter Last zeigte sich keine Veränderung dieser sehr guten Leistung. Alle Archive – auch mehrfach ineinander gepackt – wurden korrekt er-

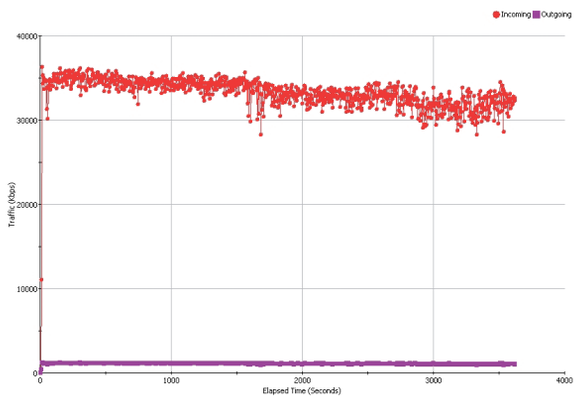

Abbildung 3: Die Langzeitmessung der HTTP-Übertragungsleistung ohne/mit Malwarelast zeigte beim Collax Security Gateway eine sehr stabile Übertragungsrate auf hohem Niveau.

kannt. Allerdings lieferte das System auch vier Fehlalarme bei HTTP, was das schlechteste Ergebnis im Testfeld war. Bei der E-Mailprüfung über POP3 gab es hingegen keine Fehlalarme, was auf eine unterschiedliche Konfiguration des Scanners für die jeweiligen Protokolle hindeutet. Zusammenfassend bescheinigen die Malware-Testergebnisse eine ordentliche Einbindung der AV-Scanner.

In Sachen Performance lieferte die Astaro-Appliance bei TCP- und HTTP-Übertragungsleistungsmessungen (inkl. der Langzeitmessungen) relativ wenig Abweichungen von einer allerdings niedrigen Durchschnittsleistung – in den Langzeitmessungen lag der mittlere Durchsatz bei 18 MBit/s. Trotz einer relativ hohen Zahl möglicher TCP-Verbindungen liegen die gleichzeitig möglichen HTTP-Verbindungen mit 3222 nur im Mittelfeld; der UDP-Durchsatz war der niedrigste im Testfeld.

Collax Security Gateway

Auch das Collax Security Gateway (Version 5.0.6) ermöglicht eine vollständige und umfangreiche Konfiguration via Webinterface. Dabei kann der Anwender zu jedem Punkt „side-by-side“ einen Online-Hilfetext einblenden lassen. Zwar erleichtern verschiedene „Wizards“ die Anfangskonfiguration, spätere Detaileinstellungen können aber dennoch teilweise etwas umständlich geraten. Die Appliance besitzt kein transparentes POP3-Proxy:

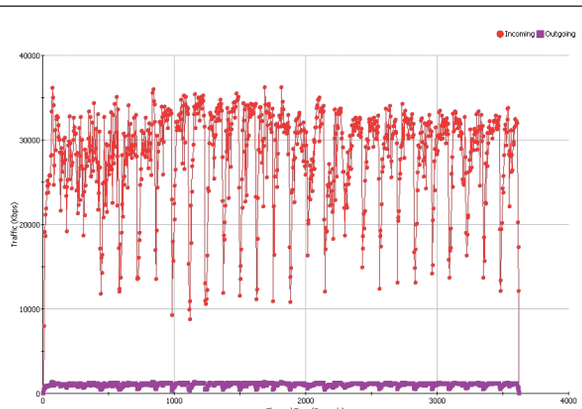

Abbildung 4: Die Langzeitmessung bei der Endian Firewall Software Appliance lieferte mit und ohne Malwarelast eine instabile Übertragungsrate mit starken Schwankungen.

Wer E-Mails mit dem AV-Scanner prüfen will, muss daher einen eigenen Mailserver betreiben, an den die Appliance geprüfte E-Mails weiterleiten kann.

Trotz vorab zugesagter Unterstützung gab es leider während der Testphase Probleme mit dem Support und der Bereitstellung von Lizenzen, sodass die Appliance nur mit dem freien ClamAV als Malware-Scanner evaluiert werden konnte, der ohne Lizenz auskommt – die mageren Erkennungsraten könnten mit einer anderen AV-Engine durchaus positiver ausgefallen sein, da ClamAV üblicherweise nicht die besten Ergebnisse liefert. Unmittelbar übertragene Malware hat das System via HTTP und POP3 in gleichem Maße gefunden – mit lediglich knapp 80 % der Wildlist lieferte sie in der genannten Konfiguration jedoch das zweitschlechteste Ergebnis im Test. Unter Last zeigte sich keine Veränderung der Erkennungsleistung – auch Fehlalarme traten keine auf.

Beim Scannen von Malware in Archivdateien kam es hingegen zu Auffälligkeiten: bei E-Mails klappte das besser als bei HTTP-Downloads – RAR-Archive zum Beispiel wurden nur aus E-Mails korrekt entpackt und gescannt. Eine weitere Kuriosität: ZIP, TAR-GZIP und TAR-BZIP werden unabhängig voneinander korrekt erkannt, wenn jedoch ein ZIP in TAR-GZIP oder TAR-BZIP steckt, findet die Appliance in E-Mails keine enthaltene Malware, bei HTTP-Traffic aber schon.

Die Ergebnisse zeigen, dass die Einbindung des AV-Scanners in die Collax-UTM an sich gut funktioniert: Es gab schließlich weder Unterschiede beim Erkennen von Malware noch bei Fehlalarmen. Die Auffälligkeit bei den Archiven deutet entweder auf eine unterschiedliche Konfiguration der Engine für die verschiedenen Protokolle oder auf eine Schwäche der E-Mailbehandlung hin, welche die Datei-Anhänge möglicherweise nicht korrekt entpacken kann. Es sei nochmals angemerkt, dass die schlechte Erkennungsleistung auf den kostenlosen ClamAV zurückzuführen ist, der im Vergleich zu anderen (kommerziellen) Virenscannern in der Regel deutlich schwächere Erkennungsraten aufweist.

Auch bei den TCP-Messungen lieferte das Collax-System ein sehr stabiles Ergebnis: Es gab kaum Abweichungen von der hohen Durchschnittsleistung. Allerdings nahm die Appliance im Kurzzeittest nach zirka 75 Sekunden Messzeit keine neuen Verbindungen mehr an: Durch die hohe Übertragungsrate und lange Time-Wait-Einstellung war möglicherweise die Verbindungstabelle vollgelaufen; das Ergebnis gibt die gemittelte Übertragungsleistung wieder.

Die HTTP-Übertragungsleistung sowie die Langzeitmessungen zeigten mittlere Werte, und zwar ebenfalls sehr stabil und ohne wesentliche Einbrüche. Den Spitzen-

wert im Testfeld lieferte die Appliance bei den gleichzeitig möglichen HTTP-Verbindungen – mit rund 51 000 waren fast dreimal so viele parallele Sessions möglich wie beim Zweitplatzierten. Auch der UDP-Durchsatz erwies sich als sehr gut.

Endian Firewall Software Appliance

Die Endian Firewall Software Appliance (Version 2.3-0) fokussiert auf die Firewallfunktion und verfügt daher über weniger umfangreiche AV-Konfigurationsmöglichkeiten, die jedoch vollständig über ein Webinterface erfolgen. Nach der Einrichtung erwies sich das System als wenig auffälliges Produkt, das im Test anstandslos seinen Dienst verrichtete.

Die Malware-Erkennung lieferte zwar keine Fehlalarme, war aber mit nur rund 77 % der Wildlist die schlechteste im Test – auch Endian setzt den kostenlosen ClamAV als AV-Engine ein. Unter HTTP lagen die Ergebnisse ein wenig besser als unter POP3, da Makroviren dort etwas besser erkannt wurden. Die Prüfung von Archiven zeigte sich ebenfalls durchwachsen: 7-Zip und ACE wurden durchweg nicht entpackt und sowohl bei HTTP als auch bei POP3 trat die gleiche Kuriosität auf, wie sie bei Collax beschrieben wurde: Malware-ZIPs in TAR-BZIP und in TAR-GZIP bleiben unerkannt.

Die Ergebnisse verdeutlichen, dass die Endian-Firewall ihren Schwerpunkt nicht auf Malware-Security legt. Die Einbindung der AV-Engine ist allerdings gut: Unter Last zeigte sich keine Veränderung der Erkennungsraten – das System behandelt zwar bei weitem nicht alle Archivformate korrekt, zeigt aber bei POP3 und HTTP konstante Leistungen, sodass dies eher dem Scanner als der Konfiguration oder dem Proxy angelastet werden kann.

Bei den TCP- und HTTP-Übertragungsleistungsmessungen ergab der Test relativ wenige Abweichungen von einer niedrigen Durchschnittsleistung. Die HTTP-Langzeitmessungen zeigen hingegen regelmäßige starke Einbrüche in der Übertragungsleistung – der errechnete Mittelwert liegt bei 26/27 MB Bit/s mit/ohne Malware-Belastung. Die gleichzeitig möglichen HTTP-Verbindungen und der UDP-Durchsatz bewegen sich im Mittelfeld des Tests.

Gateprotect

Die virtuelle Gateprotect-Appliance ist nur über eine mitgelieferte Software konfigurierbar, ein Webinterface besitzt sie nicht. Durch die naturgemäß optimale Abstimmung dieses Konfigurationsprogramms auf das Produkt, sind auch komplexe Setups einfach zu realisieren – lediglich die Menüführung ist teilweise etwas gewöhnungsbedürftig. Als Nachteil könnte man ansehen, dass

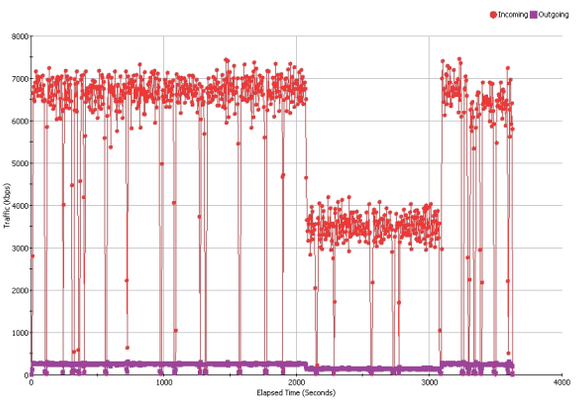

Abbildung 5: Gateprotect lieferte die besten Malwareergebnisse im Testfeld, zeigte jedoch in der Langzeitmessung instabile Übertragungsraten und einen länger währenden starken Einbruch bei AV-Belastung.

man stets diese Software zur Verfügung haben muss, um etwas an der Appliance einzustellen, da es keinerlei andere Möglichkeiten zur Konfiguration gibt – so hat man auch keine Chance, den aktuellen Status des Gerätes von einem beliebigen Arbeitsplatz im Unternehmen her aufzurufen. Das „Dashboard" in der mitgelieferten Software ist dafür jedoch auskunftsfreudig und übersichtlich.

Insgesamt macht die UTM-Appliance von Gateprotect in Sachen Malware-Scan einen sehr soliden Eindruck: Die Wildlist-Erkennung zeigte sich sowohl bei HTTP als auch über POP3 fehlerfrei, Fehlalarme traten nicht auf. Es wurden alle Archivformate korrekt erkannt, auch mehrfach ineinander gepackt. Der AV-Scanner ist von der Securityseite her gut eingebunden und zeigte auch unter Last keine Veränderung der Erkennungsleistung. Beim E-Mail-Scan (POP3) arbeitete das System jedoch sehr langsam: Teilweise brauchte der Scanner mehrere Sekunden pro Nachricht – andere Produkte waren dabei deutlich schneller. Abgesehen von Wermutstropfen in der Performance lieferte das System jedoch die besten Malware-Ergebnisse im Testfeld.

Obwohl das System mit dem UDP-Durchsatz am oberen Ende des Testfelds rangiert und bei den TCP-Übertragungsleistungsmessungen nur relativ wenig Abweichungen von einer hohen Durchschnittsleistung lieferte, zeigte es bei den HTTP-Messungen Schwächen: Sowohl in der HTTP-Übertragungsleistung als auch in den Langzeitmessungen waren sehr starke Einbrüche zu beobachten. Bei Malwarelast trat in der Langzeitmessung nach 35 Minuten ein sehr starker, fast 17 Minuten anhaltender Einbruch auf (vgl. Abb. 5). Auch die Zahl der gleichzeitig möglichen HTTP-Verbindungen ist mit nur 614 sehr niedrig.

Kerio Winroute Firewall

Die vollständige Konfiguration der Kerio Winroute Firewall sollte in der getesten Version 6.7 über die mitgelieferte Software erfolgen – über das Webinterface ist die Einrichtung etwas hakelig und nur sehr eingeschränkt

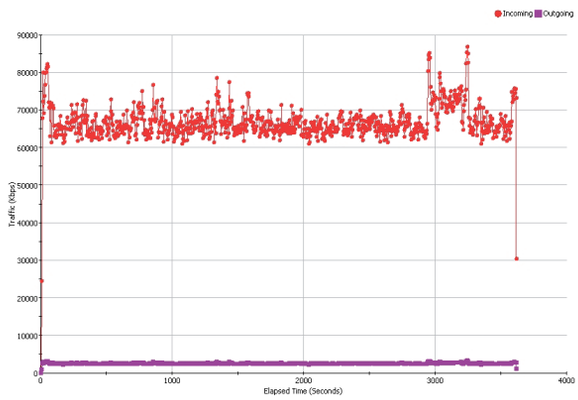

Abbildung 6: Die Kerio-Appliance lieferte sehr guten HTTP-Durchsatz, verkraftet aber nur eine relativ niedrige Zahl gleichzeitiger TCP-Verbindungen und der an sich eher hohe UDP-Durchsatz bricht bei geringer Überlast total zusammen.

möglich. Um das Produkt vernünftig einstellen zu können, benötigt man daher unbedingt das Administrationsprogramm, worauf im GUI jedoch auch hingewiesen wird. Das (Wieder-)Einspielen von Konfigurationsdaten gelang im Testaufbau nur mit Hindernissen: Hierzu galt es, den existierenden Netzwerkinterfaces diejenigen Netzwerkinterfaces zuzuweisen, die in der gespeicherten Konfiguration vorhanden waren – allerdings funktionierte das nicht zuverlässig, sodass die Interfaces anschließend noch die alten IP-Nummern hatten. Was für die Tester ein Stolperstein war, könnte in einem realen Szenario allerdings weniger schlimm sein, da derart grundlegende Konfigurationsdaten ja eher selten wechseln.

Die Malware-Erkennung erwies sich bei beiden Protokollen mit jeweils deutlich über 99 % als gut – bei POP3 leicht besser als bei HTTP. Allerdings wurden 1–2 Archivformate nicht erkannt; bei POP3 funktionierte zusätzlich ACE, in dem sich bei HTTP Malware unbemerkt verstecken konnte. Die Ergebnisse des AV-Teils hinterlassen bei der Kerio-Appliance einen insgesamt zwiespältigen Eindruck: Einerseits sind die Erkennungsraten recht hoch und immerhin wurden die meisten Archivformate zuverlässig erkannt und entsprechend behandelt. Stutzig macht aber die Tatsache, dass sich die Erkennungsleistungen bei den verschiedenen Protokollen unterscheiden: Daran ist entweder eine unterschiedliche interne Konfiguration des AV-Scanners Schuld oder die Einbindung der AV-Engine über das Proxy ist bei den Protokollen verschieden gut gelöst.

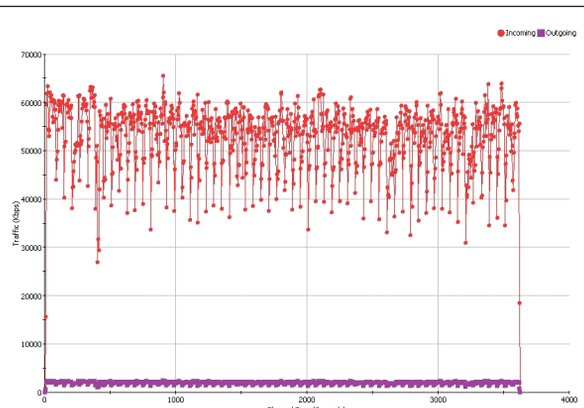

Abbildung 7: Beim XnetSolutions SXGate zeigte die Langzeitmessung der HTTP-Übertragungsleistung mit und ohne Malwarelast etliche deutliche Schwankungen.

Auch die Performancemessungen hinterließen geteilte Eindrücke: Zum einen lieferte das System den höchsten HTTP-Durchsatz im Test, HTTP-Übertragungsleistung und Langzeitmessungen zeigten einigermaßen stabile Werte und auch die Messungen der TCP-Übertragungsleistung ergaben relativ wenig Abweichungen von einer hohen Durchschnittsleistung. Die Zahl gleichzeitig möglicher HTTP-Verbindungen liegt im guten Mittelfeld. Auf der anderen Seite ist die Zahl möglicher TCP-Verbindungen ungewöhnlich stark begrenzt und der UDP-Durchsatz bewegt sich zwar am oberen Ende, zeigt jedoch schon bei geringer Überlast Stabilitätsprobleme, die zur Totalblockade von Übertragungen durch die Appliance führen. Ab Version 7, die am 1. Juni 2010 erschienen ist, heißt das Produkt „Kerio Control"; laut Hersteller wurden hierin eine umfassende Web-Administration und eine zusätzliche AV-Engine ergänzt, die auch ACE-Archive scannen können soll.

XnetSolutions SXGate

Einrichtung und Verwaltung des XnetSolutions SX-GATE (Version 5.1-1-2) erfolgen vollständig via Webinterface. Die umfangreichen Konfigurationsmöglichkeiten können zunächst etwas verwirrend sein – generell ist das Webinterface jedoch gut zu bedienen und anfängliche Schwierigkeiten der Tester wurden durch den technischen Support gut gelöst. Für viele Punkte sind zudem „Wizards" vorgesehen, welche die Grundkonfiguration des Produkts erleichtern. Nach der Einrichtung verhielt sich das SX-GATE eher unauffällig und erfüllte ohne Probleme seine Aufgaben.

Die Malware-Erkennung fand sowohl bei HTTP als auch bei POP3 fast alle Wildlist-Samples (99,9 %) und ist somit als „gut" zu bewerten. Alle Test-Archive wurden, auch mehrfach ineinander gepackt, fehlerfrei erkannt. Allerdings gab es zwei Fehlalarme, sowohl bei HTTP als auch bei POP3.

Die XnetSolutions-Appliance ist von der AV-Seite her ein sehr solides Produkt: Die reine Erkennungsleistung landet zwar nur auf dem dritten Platz, allerdings sind die Ergebnisse für POP3 und HTTP identisch, alle Archivformate wurden korrekt verarbeitet und auch unter Last zeigten sich keine Veränderung der Erkennungsleistung – die Einbindung der AV-Engine in die UTM-Appliance ist also sehr gut gelöst. Die Fehlalarme trüben dieses gute Bild ein wenig: Da davon auszugehen ist, dass eine Appliance überwiegend mit gutartigen E-Mails und Webseiten „gefüttert" wird, sollte man diesen Punkt nicht unterbewerten.

Bei der TCP-Übertragungsleistung lieferten die Messungen relativ wenig Abweichungen von einer hohen Durchschnittsleistung. Wie bei der Collax-Appliance meldete das Testsystem auch hier nach zirka 75 Sekunden die Nicht-Annahme neuer Verbindungen, sodass diese Werte entsprechend gemittelt sind. Auch hier liegt die Vermutung nahe, dass durch die hohe Übertragungsrate und lange Time-Wait-Einstellung möglicherweise die Verbindungstabelle voll war.

Die HTTP-Übertragung sowie die Langzeitmessungen zeigten eine gute Leistung, die jedoch mit regelmäßigen Einbrüchen durchsetzt war. Der gemittelte Wert liegt aber dennoch auf Platz Zwei im Testfeld und auch der UDP-Durchsatz bewegt sich am oberen Ende. Mit nur 384 gleichzeitig möglichen HTTP-Verbindungen erzielt das System in dieser Kategorie allerdings gleichzeitig das schlechteste Ergebnis im Test. Laut Hersteller sollen zwischenzeitlich erfolgte Optimierungen in der aktuellen Version eine bessere Leistung ermöglichen.

Fazit

Auch virtualisierte UTM-Appliances können eine gute Schutzwirkung und eine vertretbare Performance haben – da Sicherheit letztlich ein Dienst unter vielen anderen ist, dürften solche Lösungen vor allem an denjenigen Standorten Einzug halten, an denen sowieso schon virtualisiert wurde oder wird.

Sowohl die Malware-Erkennungsraten nebst Fehlalarmen als auch die Performance streuten im Test über einen weiten Bereich: Die Leistung der Appliances bricht je nach Hersteller durch die Überprüfung der HTTP-Daten auf zirka 1–15 % gegenüber ungeprüften TCP-Daten ein. Allem voran zeigte die Konstanz der HTTP-Übertragungsleistung deutliche Unterschiede zwischen den Herstellern.

Alles in allem ergab sich kein klarer Testsieger, sondern die getesteten Systeme hatten sowohl ihre Stärken als auch Schwächen, sodass die Auswahl der passendsten virtualisierten Appliance stark vom jeweiligen primären Einsatzzweck sowie der ergänzenden Sicherheitsinfrastruktur abhängen dürfte. ■

Prof. Dr. Bernhard Stütz ist Leiter des Zentrums für Informations- und Kommunikationstechnik der FH Stralsund sowie des Steinbeis-Transferzentrums Projektierung und Evaluierung von Netzwerken (www.stz-netze.de). Thomas Rottenau ist Leiter Testlabor bei STZ Netze, Stralsund. Guido Habicht ist Geschäftsführer, Maik Morgenstern Technischer Leiter bei der AV-Test GmbH, Magdeburg (www.av-test.org).

Über die Tester

Mit mehr als 15 Jahren Tätigkeit im Bereich Virenforschung und Datensicherheit ist die **AV-Test GmbH** (www.av-test.de) ein erfahrener Anbieter von IT-Sicherheitstests und Consultingdienstleistungen. 2004 von Andreas Marx, Oliver Marx und Guido Habicht in Magdeburg gegründet, unterlag sie seither stetigem Wachstum und umfasst inzwischen 14 Mitarbeiter. Jährlich werden mehr als 2 500 Einzeltests von Anti-Viren- und Anti-Spyware-Software, Personal Firewalls sowie verwandten Produkten im Auftrag von Herstellern, Integratoren (OEM), Firmenkunden und Zeitschriften durchgeführt. Eine moderne Ausstattung in den Testlaboren mit mehr als 200 Client- und Server-Systemen sowie 140 TByte Malware- und Testdateien ermöglichen sowohl komplexe Testszenarien für Einzelprodukte und technische Komponenten als auch vergleichende Analysen.

Das **Steinbeis Transferzentrum (STZ) „Projektierung und Evaluierung von Netzwerken“** (www.stz-netze.de) wurde 1998 an der Fachhochschule Stralsund von Prof. Dr. Stütz gegründet. Im Mittelpunkt der Aktivitäten steht die Entwicklung von Testmethodiken zur Qualität von Netzwerken und ihren Komponenten – vor allem das Echtzeitverhalten wird untersucht, da dieses über die Verwendbarkeit eines Netzwerks zur Durchleitung von Sprach- und Videodiensten entscheidet. Die Ergebnisse der Untersuchungen von Netzwerkkomponenten werden regelmäßig in Fachzeitschriften veröffentlicht. Die so gewonnene Erfahrung nutzt STZ zudem in Consultingprojekten, um Kunden bei der Planung, Ausschreibung und Inbetriebnahme von Netzwerklösungen zu unterstützen. Das Labor hat Zugriff auf Netzwerkmesstechnik für Datenraten im zweistelligen Gigabitbereich.

Wir bedanken uns bei der Firma **Thomas Krenn** für die Bereitstellung zweier virtualisierter Server und der Firma **Spirent** für die messtechnische Unterstützung durch einen Lastgenerator/Analysator Smartbits 6000C sowie den Systemen Spirent Avalange und Reflector 2500.

Hersteller	Astaro
Anschrift	An der RaumFabrik 33a
	76227 Karlsruhe
	Deutschland
Ansprechpartner	k. A.
Telefon	+49 721 25516-0
Fax	+49 721 25516-200
E-Mail	emea@astaro.com
Web	www.astaro.de
Produkt	**Astaro Security Gateway**
getestete Version	7.501
Leistungsumfang[1]	
Stateful-Inspection-Firewall	ja
Application-Level-Gateway (Firewall)	ja
VPN-Gateway	IPsec, SSL, L2TP, PPTP
Intrusion Detection/Prevention	ja
Anti-Malware	HTTP, POP3, SMTP, FTP, HTTPS
Anti-Spam	ja
URL-/Inhaltsfilter (HTTP)	ja
Data Leakage/Loss Prevention	nein
SSL-Proxy für Inhaltsprüfungen	ja
virtuelle Poststelle[3]	nein
Sonstiges	Active/Active-Cluster, IM- und P2P-Control, E-Mail-Encryption, 2 AV-Scanner
Lizenzkosten[2] **(Anschaffung/jährlich)**	
für 50 Nutzer	2015/1915[4]
für 250 Nutzer	6330/6014[4]
Malware-Messungen	
Wildlist-Erkennungsrate	
via HTTP	100,0 %
via HTTP unter HTTP-Last	100,0 %
via POP3	100,0 %
Malware-Erkennung in Archiven	
via HTTP	6/6
via POP3	6/6
Fehlalarme	
via HTTP	1,0 %
via POP3	0,0 %
Performance-Messungen	
UDP-Durchsatz [Mbit/s]	
IMIX	<100
Rahmengröße 1518	<200
Rahmengröße 1024	<200
Rahmengröße 512	<100
Rahmengröße 256	<100
Rahmengröße 64	<100
TCP-Übertragungsleistung [Mbit/s]	149
HTTP-Übertragungsleistung [MBit/s]	
Kurzzeitmessung	19
Langzeitmessung ohne Malware-Last	18
Langzeitmessung mit Malware-Last	18
gleichzeitig mögliche Verbindungen	
TCP	59.464
HTTP	3.222

[1] nach Firmenangaben
[2] Zirkapreise nach Firmenangaben
[3] zur zentralen Ver-/Entschlüsselung und Signatur von E-Mails

Collax	Endian	Gateprotect	Kerio	XnetSolutions
Osterfeldstraße 86	Via Pillhof 47	Valentinskamp 24	Brückenstr. 2	Benzstraße 32
85737 Ismaning	39010 Frangarto	20354 Hamburg	51379 Leverkusen	71083 Herrenberg
Deutschland	Italien	Deutschland	Deutschland	Deutschland
Falk Krämer	Robert Wendel	Kai Bulau	Arndt Stubbe	Inge Schmidt
+49 89 990157-0	+49 8106 30750-13	+49 1805 428377	+49 2171 3636136	+49 7032 95596-0
+49 89 990157-11	+49 8106 30750-29	+49 1805 428332	+49 2171 3636131	+49 7032 95596-25
info@collax.de	germany@endian.com	info@gateprotect.de	info@kerio.de	inge.schmidt@xnetsolutions.de
www.collax.de	www.endian.com	www.gateprotect.de	www.kerio.de	www.xnetsolutions.de
Collax Security Gateway	**Endian Firewall Software Appliance**	**Gateprotect xUTM Virtual Appliance**	**WinRoute Firewall[6]**	**SX-GATE**
5.0.6	2.3-0	8.5	6.7.1 (6399)	5.1-1-2
ja	ja	ja	ja	ja
ja	ja	ja	ja	ja
IPsec, clientless SSL, L2TP, PPTP	IPsec, OpenVPN	IPsec, SSL, PPTP	clientless VPN oder Custom-VPN (incl. Client-Sw.)	IPsec, L2TP over IPsec, OpenVPN
ja	ja	ja	ja (ab Ver. 7)	ja
HTTP, POP3	HTTP, POP3, SMTP, FTP	HTTP, POP3, SMTP, FTP, HTTPS	HTTP, POP3, SMTP, FTP	HTTP, POP3, SMTP, FTP
ja	ja	ja	nein	ja
ja	ja	ja	ja	ja
ja	nein	nein	nein	nein
nein	nein	ja	nein	ja
nein	nein	ja	nein	nein
VoIP-Support (SIP, RTP), Traffic-Shaping, Tagged VLAN, Bridging, Active-Directory-(AD)-Anbindung, USV-Unterstützung	Quality-of-Service, Hotspot, High-Availability, Multi-WAN, zentr. Mgmt., optional: AV von Sophos, Anti-Spam von Commtouch	Bandbreitenmanagement (inkl. Traffic Shaping und QoS), „eGUI Technologie" (zur graf. Admin.)	Stat./Reporting bis auf Benutzerebene, Active-Directory-(AD)-Integration, Dual AV + Clam-AV-Proxy, Link-Load-Balancing, Fail-Over, Bandwidth-Limiter	Proxies für SMTP, POP3, FTP, SIP, HTTP(S) und OWA, Reverse-HTTP-Proxy, policy-based Routing
0/860	0/625	1197/429[5]	935/281	1650/396
0/1465	0/1995	3777/1347[5]	4295/1289	3180/763
80,0 %	77,0 %	100,0 %	99,7 %	99,9 %
80,0 %	77,0 %	100,0 %	99,7 %	99,9 %
80,0 %	77,0 %	100,0 %	99,9 %	99,9 %
3/6	4/6	6/6	4/6	6/6
4/6	4/6	6/6	5/6	6/6
0,0 %	0,0 %	0,0 %	0,0 %	0,5 %
0,0 %	0,0 %	0,0 %	0,0 %	0,5 %
<400	<300	<400	<400	<400
1000	<900	1000	<700	1000
<900	<600	<900	<700	<800
<500	<300	<500	n/a	<400
<300	<200	<300	n/a	<300
<100	<100	<100	n/a	<100
565	193	556	479	556
35	35	6	73	59
31	27	5	70	54
30	26	5	62	48
65.536	64.512	64.511	5.928	64.502
51.162	16.326	614	3.333	384

[4] inkl. aller Subscriptions – kostenlose „Essential Firewall" auch für Unternehmen verfügbar

[5] bei Nutzung mit 3-Jahre-UTM-Package (Anti-Spam/-Malware und Webfilter)

[6] Nachfolgeprodukt seit 1. Juni 2010: Kerio Control, Ver. 7.0, neu mit IDS/IPS und integriertem Sophos-AV

Sind Sie verantwortlich für die IT-Sicherheit?

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit
Zutrittskontrolle
Virenabwehr
Verschlüsselung
Risikomanagement
Abhör- und Manipulationsschutz
Sicherheitsplanung
Elektronische Signatur und PKI

<kes> ist seit 20 Jahren *die* Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche, viele interessante Links, Stichwort-Lexikon IT-Security-Begriffe, Verzeichnis relevanter Veranstaltungen und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

PROBEHEFT-ANFORDERUNG

☐ **ja,** bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Das Abonnement beinhaltet ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info

Datum | Zeichen | Unterschrift

Lieferung bitte an

Telefon Durchwahl

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim