Intrusion Prevention – neue Ansätze der Computersicherheit

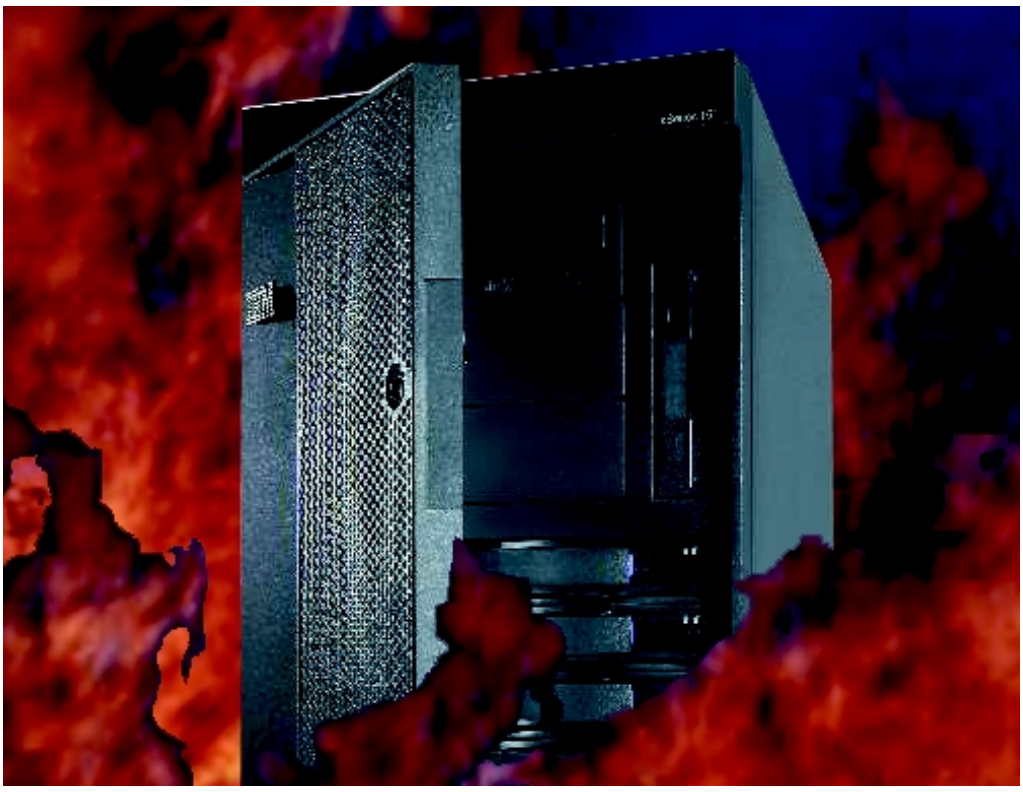
* Marc Ruef

Das Thema der Computer- und Netzwerksicherheit beschäftigt ganze Industrien. Mit der Hilfe klassischer Schutzmechanismen – wie Antiviren-Software, Firewalling- und Intrusion-Detection-Systeme – werden moderne Netzwerke abgesichert. Eine typische Methode des Erkennens von Angriffen ist durch das Pattern-Matching gegeben. Hierbei wird – ob für Antiviren- oder Intrusion Detection – Ausschau nach verdächtigen Zeichenketten gehalten, die als Indiz für eine drohende Gefahr gewertet werden. In diesem Artikel werde ich auf die Nachteile des Pattern-Maching eingehen und Lösungen im Sinn der Angriffsprävention aufzeigen.

Vor einiger Zeit war ich in eine Diskussion verwickelt, in der mich mein Gegenüber mit seiner Liebe zur Wahrheit buchstäblich überrumpelt hat. Seiner Ansicht nach sei das Bemühen um Computersicherheit ein utopisches Unterfangen, denn die Angreifer seien der Branche stets einen Schritt voraus. Wenn ich mir die letzten Jahre vergegenwärtige, welche Techniken und Methoden die IT-Branche zur Wahrung und Stärkung der Systemsicherheit hervorbrachte, so liegt man nicht falsch, vertritt man diese Meinung. Bestes Beispiel sind die Antiviren-Lösungen, die auf Pattern-Matching basieren.

Sind wir in der Lage den Mail-Attachments den Zugriff zu verbieten, schneiden wir dem Wurm und seinen Verwandten die Luft ab.

Gehen wir davon aus, dass ein 16-jähriger Schüler aus purer Langeweile einen Computervirus programmiert, der sich dank einigen ungeschickten Sicherheitseinstellungen in einer gängigen Mailsoftware selbstständig weltweit innerhalb weniger Stunden zu verbreiten in der Lage ist. Dieses korrupte Programm pflegt in die Betreffzeile der sich selber mittels Mails verschickten Replika die Worte "I LOVE YOU" zu schreiben.



Die Hersteller von Antiviren-Software werden früher oder später auf den Wurm aufmerksam, der sich mit rasender Geschwindigkeit durch die Mailserver des Internets schlängelt. Sie versuchen so schnell wie möglich ihrer Antiviren-Software beizubringen, diesen Schädling zu erkennen, um den durch ihn möglichen Schaden zu minimieren. Dabei wird versucht, mit der Hilfe eines oder mehrerer eindeutiger Merkmale das bösartige Programm zu identifizieren. Da sich die Software stets mit den Worten "I LOVE YOU" in der Betreffzeile verbreitet, ist es ein Leichtes, E-Mails, die diese Charakteristik aufweisen, als potentiellen ILOVEYOU-Wurm zu klassifizieren.

Die Grenzen des Pattern-Matchings

Die am Beispiel des ILOVEYOU-Virus gezeigte Pattern-Matching-Technologie bringt zwei enorme Nachteile mit sich. Als erstes muss man sich den Prozess vor Augen halten, der durchlaufen werden muss, bis das Pattern-Matching als erfolgreiche Gegenmassnahme zum Einsatz kommen kann:

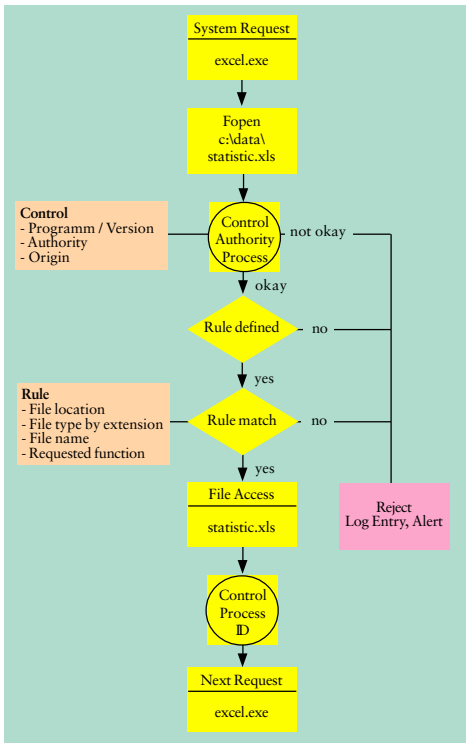


Abbildung 2: Das Entscheidungs-Modell.

1. Die bösartige Software muss als solche bekannt werden.
2. Danach gilt es eine Identifikation an mindestens einem eindeutigen Merkmal zu ermöglichen.
3. Dabei liegt die Schwierigkeit darin, dass alle Schädlinge erkannt werden und solche, die nur ähnlich aussehen, ignoriert werden.
4. Zum Schluss müssen sämtliche Signaturen der Antiviren-Lösungen ein Update durchführen, um gegen den neuen Schädling immun zu sein.

Das zweite Problem ist eines, das von vielen Leuten unterschätzt und von der Branche gerne totgeschwiegen wird: Die Gratwanderung zwischen zu restriktivem und zu laxem Pattern-Matching stellt eine schier utopische Aufgabe dar. Jeder, der sich schon einmal in einem Programmier-Projekt um ein solides Pattern-Matching bemüht hat, der weiss um die Probleme dieses Unterfangens. Ebenso werden viele Administratoren nervös, wenn man ihnen mit einer Anpassung des Regelwerks ihres Intrusion-Detection-Systems droht. Beim Pattern-Matching eine unverbesserliche Perfektion zu erreichen, diese Aufgabe hielt schon so

All in one-Lösungen

Firewall-Systeme, Antiviren-Software und Intrusion Detection-Lösungen, das sind die heutigen Ansätze, Netzwerke abzusichern. Für viele Leute scheint diese Aufgabe einfach, denn nach dem Entscheid und Kauf einer entsprechenden Lösung erwarten sie ein Höchstmass an Sicherheit für ihre Umgebung. Doch dies ist ein Trugschluss, wie Vorkommnisse der letzten Jahre ganz offensichtlich zeigen. Sämtliche Sicherheitslösungen scheitern am ehesten an einer fehlerhaften Konzeption und der daraus resultierenden mangelhaften Umsetzung. Es soll aber auch erwähnt werden, dass oft die Lösungen in eine Situation gepresst werden wollen, für die sie gar nicht geschaffen wurden. So beginnen die Firewall-Hersteller mit der Implementierung von Antiviren-Mechanismen und die Entwicklung von Intrusion Detection-Systemen bewegt sich immer mehr Richtung Firewalling.

Ein Grundsatz von Sicherheitslösungen besagt, dass sie so einfach wie möglich gehalten werden sollen. Dadurch will das Risiko eines Fehlers – ob bei der Entwicklung oder im Betrieb – minimiert werden. Zusätzliche Features bei Firewall-Lösung sind genau das Gegenteil dieses Axioms. Die Chance, dass das Firewall-System selbst gegen Angriffe verwundbar ist, steigt mit den durch sie gewährten Möglichkeiten.

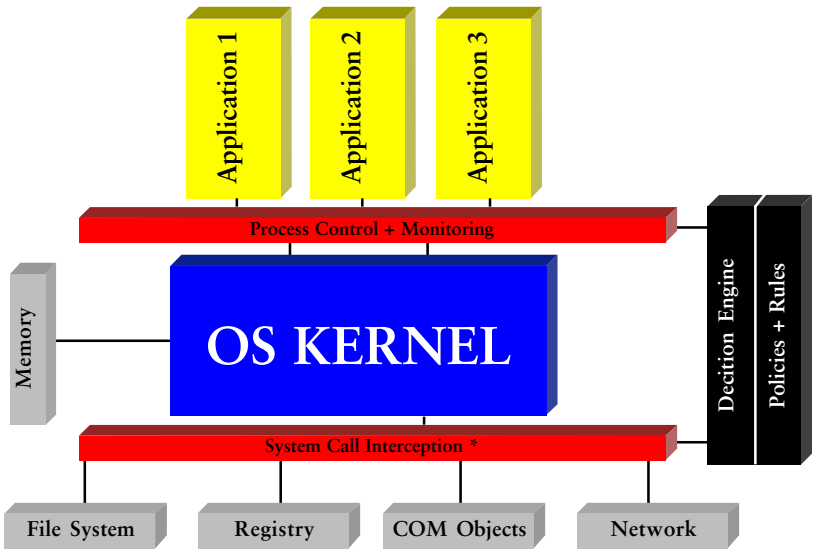


Abbildung 1: Die Shim-Technologie. *Systems-Call Interception ermöglicht die vollständige Kontrolle der Applikationszugriffe auf alle System-Funktionen und Ressourcen nach dem "Intrinsic-Prinzip" von innen heraus; Funktionen werden explizit für die spezifischen Applikationen erlaubt.

manchen Mathematiker und Programmierer vom Schlafen ab.
Schauen wir uns einmal an einem Beispiel an, inwiefern dies wirklich ein Problem darstellt. Kehren wir zurück zu unserem Beispiel, in dem sich der Computervirus per Mail verschickt. In diesen ausgehenden, infizierten Mails ist stets die Betreffzeile "I LOVE YOU" vorhanden. Wir müssten nun also ein simples Pattern-Matching realisieren, das die Existenz der folgenden Merkmale bemerkt und entsprechend Alarm schlägt:

- Beim Datenverkehr handelt es sich um E-Mail (z.B. TCP-Port 25 oder 110).
- Es ist die Betreffzeile "I LOVE YOU" enthalten.

Dies ist wahrlich keine sonderlich schwere Aufgabe. Nun, was passiert jedoch, wenn der Wurm mit der Eigenschaft zur Polymorphie entwickelt wurde? Dies bedeutet, dass er sich im Laufe seines Verbreitungszyklus verändert. Äussern kann sich dies durch die Wahl verschiedener Betreffzeilen. So wird aus dem "I LOVE YOU" plötzlich ein "I MISS YOU" oder "I SEEK YOU". Logische Konsequenz einer solchen Veränderung ist, dass unser Pattern-Matching für die Wortkette "I LOVE YOU" nicht mehr greifen kann. Ergo sind wir nicht mehr in der Lage, den Virus zu erkennen und Alarm zu schlagen.

Einen Schritt weiter mit Intrusion Prevention

Eine der Ideologien von Intrusion Prevention ist, dass die beiden Nachteile des Pattern-Matchings

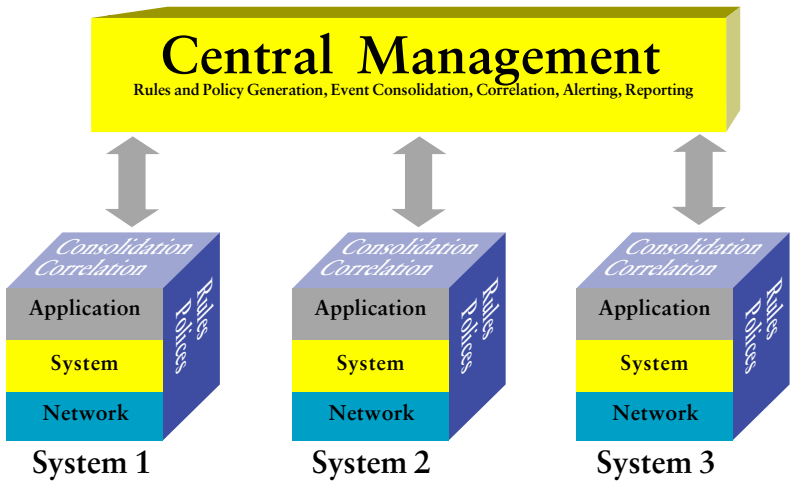


Abbildung 3: Die Administrations-Architektur.

wegfallen. Die Vorlaufzeit, bis ein Angriff als solcher identifiziert wird, seine Merkmale extrahiert werden und ein Pattern kreiert wird, ist nicht mehr nötig. Zu Beginn werden dem Betriebssystem und der darauf laufenden Anwendungen ihre Grenzen aufgezeigt. Nehmen wir einmal mehr das Beispiel des ILOVEYOU-Wurms. Dieser repliziert sich so, dass ein Attachment, das mit dem ILOVEYOU-Mail verschickt wird, automatisch von den Outlook-Clients ausgeführt wird. Sodann werden aus dem lokalen Adressbuch sämtliche Einträge ausgelesen und eine Replika von sich selbst (Mail mit Attachment) weiterverschickt.
Sind wir in der Lage, grundsätzlich sämtlichen Mail-Attachments den Zugriff auf sensitive Daten – in diesem Falle das lokale Adressbuch – zu verbieten, so schneiden wir dem ILOVEYOU-Wurm und seinen Verwandten die Luft ab. Sodann ist es unabhängig, ob der nächste Mail-Wurm die Betreffzeile "I MISS YOU" wählt oder sich für eine pseudo-zufällige Betreffzeile entscheidet. Die normale und gewünschte Funktionalität des Mailprogramms (und der Attachments) wird dadurch nicht behindert. Auch weiterhin können Word-Dokumente verarbeitet werden und lassen sich Bilder anschauen.

Wie funktioniert Intrusion Prevention

Wenn wir ein Betriebssystem oder eine Software einsetzen wollen, so lassen wir uns oft von den gegebenen Möglichkeiten begeistern. Hört man einen Windows- und einen Linux-Benutzer streiten, so dreht es sich in erster Linie um die Frage, welches System denn nun mehr könne. Aus der Sicht der Sicherheit ist dies absolut unsinnig (okay, nicht ganz, wenn man bedenkt, dass es ein zusätzliches Feature sein kann, dass man mehr Möglichkeiten in Punkto Sicherheit hat): Je mehr Möglichkeiten ein Betriebssystem bietet, desto komplexer ist die interne Verarbeitung und teilweise auch die Bedie-

Über den Autor

Marc Ruef arbeitet als Security Consultant bei der Firma Inter-Networking AG in Dietikon. Er ist dort in erster Linie für Security Auditings und Assessments zuständig. Im September dieses Jahres erschien im Data Becker Verlag sein erstes Buch zum Thema Computersicherheit mit dem Titel "Hacking Intern" (ISBN 381582284X).

nung. Je komplexer eine Lösung ist, desto grösser ist die Chance, dass bei der Entwicklung oder im Betrieb ein Fehler unterläuft. Dies kann von programmiertechnischen Pufferüberläufen bis hin zu gutgläubigen Konfigurationsfehlern reichen. Fakt ist, dass eine Vielzahl an Möglichkeiten automatisch eine grössere Angriffsfläche bietet.

Die amerikanische Firma Okena hat eine Software entwickelt, die nicht mehr mit diesen Signatur-Problemen zu kämpfen hat. Das Konzept dieser Lösung ist einfach und genial zugleich. Moderne Betriebssysteme arbeiten alle nach demselben Prinzip. Eine jede Software hat für das Nutzen der Ressourcen des Computers den Betriebssystem-Kernel zu fragen. Durch diese System-Calls wird von Dateizugriffen über die Speicherzuordnung bis hin zur Rechenleistung alles koordiniert.
StormWatch setzt auf die so genannte "Shim-Technologie". Ein Shim (dt. Messplättchen) ist in diesem Zusammenhang ein Software-Agent, der auf dem zu schützenden System installiert wird. Dieses Plugin beobachtet sämtliche Kernel-Kommunikationen, die durch die Software auf dem System getätigt werden.
Bei der Intrusion Prevention gehen wir so vor, dass unnötige Mechanismen und Möglichkeiten von Systemen unbrauchbar gemacht, indirekt abgeschaltet werden. So muss man sich fragen, ob es überhaupt für meine Mail-Applikation möglich sein soll, auf sensitive Betriebssystem-Daten (z.B. Passwort-Dateien) zugreifen zu können. Ein trojanisches Pferd, das automatisiert versucht, die heiklen Daten per Mail zu verschicken, wird scheitern, denn der entsprechenden Mail-Anwendung werden sämtliche Zugriffsrechte entzogen.

Praxisbeispiel an einem Webserver

Mehr Möglichkeiten bietet Intrusion Prevention jedoch auf Server-Systemen, die Dienste zur Verfügung stellen und mit Benutzern interagieren müssen. Nehmen wir als zweites Beispiel einen MS IIS, der 24 Stunden die Firmen-Webseite bereitstellen können muss.
Die meisten Netzwerkprotokolle wie auch das Hyper Text Transfer Protocol basieren auf dem Client/-Server-Prinzip. Der Client initialisiert eine TCP-Verbindung an den Webserver, wo er danach seine Anfrage absetzt. Die übliche Form hierzu ist "GET /index.html". Diese Datei befindet sich im Wurzelverzeichnis des Webservers. Bei einem MS IIS ist dies im Normalfall die "C:\Inetpub\wwwroot". Wir rufen also eigentlich die Datei "C:\Inetpub\wwwroot\index.html" ab. Ist das Dokument vorhanden und dem Webserver ist die Herausgabe dessen erlaubt, schickt er den http-Statuscode "200 OK" und den Inhalt der Datei /index.html zurück.
Eine typische Angriffsmöglichkeit besteht nun darin, dass der Webserver dazu überlistet wird, Dateien herauszugeben, für die eigentliche kein Zugriff möglich sein sollte. Bei den meisten Betriebssystemen kann durch zwei aufeinander folgende Punkte in der Angabe eines Pfads eine Hierarchie-Stufe höher gesprungen werden. Wir können nun versuchen mit diesem Trick während einer http-Sitzung mit einem Webserver durch die Verzeichnisstruktur des Systems zu hüpfen. Ist der Webserver gegen diese Art von Angriff verwundbar, so kann mit dem http-Kommando "GET ../../winnt/repair/sam._" die Passwort-Datenbank des Windows-Systems ausgelesen werden und damit grösseren Unfug zu treiben.
Wenn wir während dieses Angriffs die Prozesstabelle des attackierten Rechners im Auge behalten, so bemerken wir, dass der Prozess inetinfo.exe – das Kernstück des MS IIS – für den ungewollten Dateizugriff verantwortlich war. Jetzt können wir uns die gleiche Frage stellen, wie beim Beispiel des Mail-Clients: Muss dem Webserver-Dämon ein Zugriff auf sensitive Systemdateien erlaubt werden? Die Antwort wird in den meisten Fällen nein lauten. Mit der Hilfe von Werkzeugen wie dem Okena StormWatch sind wir nun in der Lage, dem Programm inetinfo.exe nur Zugriffe auf Web-Dokumente wie *.html*.jpg, die sich im Webserververzeichnis befinden, zu erlauben. Alle anderen Zugriffe werden verhindert. Sodann macht es keinen Unterschied mehr, ob die Webserver-Applikation dahingehend ausgetrickst werden kann, dass sie einem die gewünschten Daten liefert: Zugriffe auf sensitive Informationen

Literaturverzeichnis

Beck, Michael / Böhme, Harald / Dziadzka, Mirko [1999], Linux Kernelprogrammierung – Algorithmen und Strukturen der Version 2.2, Addison-Wesley, München, ISBN 3827314763

Brummermann Hendrik [2002], Wie Personal Firewalls ausgetrickst werden können, http://www.computec.ch/dokumente/firewalling/pf-umgehen/pf-umgehen.html

Departement of Defense [20. Juli 2000] "ILOVEYOU" Virus Lessons Learned Reports, http://call.army.mil/io/ll/love.pdf

Gieseke, Wolfram / Rogge, Marko / Ruef, Marc / Velten, Uwe [September 2002], Hacking Intern, Data Becker, Düsseldorf, ISBN 381582284X

McClure, Stuart / Scambray, Joel / Kurtz, George [26. September 2001], Hacking Exposed – Network Security Secrets & Solutions, 3rd Edition, McGraw-Hill Companies, ISBN 0072193816, deutsche Ausgabe, Das Anti-Hacker-Buch, MITP Verlag

McKusick, Marshall Kirk / Bostic, Keith / Karels, Michael J. [1996], The Design and Implementation of the 4.4BSD Operating System, Addison Wesley Publishing Company, ISBN 0201549794

sind vom Betriebssystem-Kernel her nicht mehr möglich.

Fazit

Das Beispiel des sicheren Webservers hat gezeigt, wie einfach und kompetent unerlaubte Schreibzugriffe unterbunden werden können. Selbst die unzähligen Varianten eines Angriffs können erkannt werden, da schlussendlich alle früher oder später beim Kernel anklopfen müssen, um die notwendigen Rechte einzuholen (vgl. McKusick et al 1996). Ein Absichern des Systems ist auf einer sehr tiefen Ebene möglich.
Dieses Hardening beschränkt sicher nicht nur auf unerlaubte Schreibzugriffe durch kompromittierte oder bösartige Software. Da auch die einzelnen Hardware-Komponenten (z.B. Netzwerkkarte) auf das Zusammenspiel mit dem Kernel des Betriebssystems angewiesen sind, können auch dort sehr feine Abstufungen bezüglich der Privilegien gemacht werden.
Vom Grundprinzip her ist mit Intrusion Prevention alles möglich, was man auf Software-Ebene mit einem Betriebssystem anstellen kann. Und dies ist schlussendlich der grösste Nachteil einer solchen Lösung. Das Herausfinden, welche Funktionen eine Software für den Betrieb benötigt, ist unter Umständen eine langwierige Aufgabe. Das Anpassen eines Mail-Clients oder einer Webserver-Software ist durchaus in einem angemessenen Zeitrahmen zu bewältigen. Grössere Systeme, wie zum Beispiel umfängliche MS-Exchange oder komplexe Oracle Datenbanken, stellen jedoch eine ungemeine Herausforderung dar.
Okena StormWatch ist ein starkes Sicherheits-Werkzeug, dessen Möglichkeiten schier unbegrenzt sind, denn es wird am wichtigsten Punkt eines jeden Systems angesetzt: Dem Kernel selbst. Wer den Kernel beherrscht, der hat die Macht über das gesamte System.

StormWatch

Das von der amerikanischen Firma Okena herausgegebene Produkt StormWatch ist die erste marktreife Intrusion Prevention-Lösung. Einfache Bedienbarkeit, die selbst den Einsatz in einem grösseren Umfeld ermöglichen, zeichnen die Software aus. StormWatch arbeitet nach dem Manager/Agent-Prinzip: Der Manager ist die zentrale Stelle, die die auf den zu schützenden Systemen installierten Agents konfiguriert und überwacht. Zu bedienen ist das Management-Interface mit einem herkömmlichen Webbrowser. Die Agents sind für Windows- und Unix-Systeme erhältlich.

Weitere Informationen

http://www.okena.com
In der Schweiz ist die Firma Inter-Networking AG für den Verkauf und Vertrieb von Okenas StormWatch zuständig.
http://www.internetworking.ch

Weiterführende Informationen zu Computersicherheit
http://www.computec.ch