

**Benutzerfreundlichkeit erhöht die Sicherheit**

## Firewalls mit Bedienkomfort

Was wären Formel-1-Piloten ohne elektronisches Cockpit? Gute Autofahrer, die nur mit Glück ihre Rennmaschinen beherrschen. Moderne Firewalls sind so komplex, dass ihre Administrierbarkeit zum Sicherheitsrisiko zu werden droht. Neue Bedienkonzepte wirken dieser Gefahr entgegen.

In Zeiten knapper Investitionsbudgets hat sich das Thema Ergonomie längst zum Kostenargument entwickelt. Allerdings stellt sich die Frage, ob dieser Aspekt auf die Welt der Firewalls übertragbar ist. Zwar werden diese Sicherheitslösungen immer komplexer, aber ihre Administratoren sind in der Regel IT-Profis, für die Befehlszeilen und Code eine vertraute, lieb gewonnene Welt darstellen. Doch ist das immer die beste Wahl?

Im Zeitalter des E-Business gleichen sich die Unterschiede bei den Sicherheitsniveaus in Abhängigkeit von der Firmen- und Netzgröße immer mehr an. Darauf gibt es prinzipiell nur zwei verschiedene Antworten: die Zahl der IT-Administratoren signifikant zu erhöhen oder die Administration zu vereinfachen.

Wer letzteres will, muss den Menschen, seine Vorstellungen und Erwartungen in den Mittelpunkt seiner Überlegungen zur Gestaltung der Administrationskonsolen von Firewalls machen.

### Fünf Gebote der Ergonomie

Anhaltspunkte für die Qualität der Ergonomie von Firewall-Cockpits liefern die Dialogprinzipien zur ergonomischen Softwaregestaltung, wie sie in der internationalen Norm ISO 9241, Teil 10 formuliert sind.

### Ein Bildschirmdialog muss „aufgabenangemessen“ sein.

Diese Regel bedeutet unter anderem, dass unnötige Arbeitsschritte vermieden oder

vom System automatisch ausgeführt werden sollten. Außerdem sollten nur diejenigen Informationen angezeigt werden, die unmittelbar mit der vorliegenden Aufgabe zusammenhängen. Herkömmliche Bedieneroberflächen von Firewalls stellen die verschiedenen Features und vielleicht noch die Beziehungen der verschiedenen Einstellungen untereinander dar. Dies nützt aber wenig, wenn ein Administrator einen neuen Benutzer anlegen will, der im Vertrieb arbeitet und daher den gleichen Sicherheitsregeln unterworfen sein soll wie seine Abteilungskollegen. Eine „aufgabenangemessene“ Bedieneroberfläche stellt deshalb den neuen Benutzer und die Anwendergruppe, der er zugeordnet werden soll, dar. Per Drag and Drop wird das Symbol des neuen Users in die Gruppe integriert und erbt automatisch deren Sicherheitseinstellungen. Sollen für diesen Anwender, weil es sich zum Beispiel um den neuen Vertriebsleiter handelt, teilweise abweichende Regeln gelten, so sollte ein Mausklick auf das Symbol des Users genügen, um alle für ihn relevanten Funktionalitäten der unterschiedlichen Firewall-Applikationen und ihre aktuellen Konfigurationen in einer konsolidierten Darstellung anzuzeigen. Die Änderun-

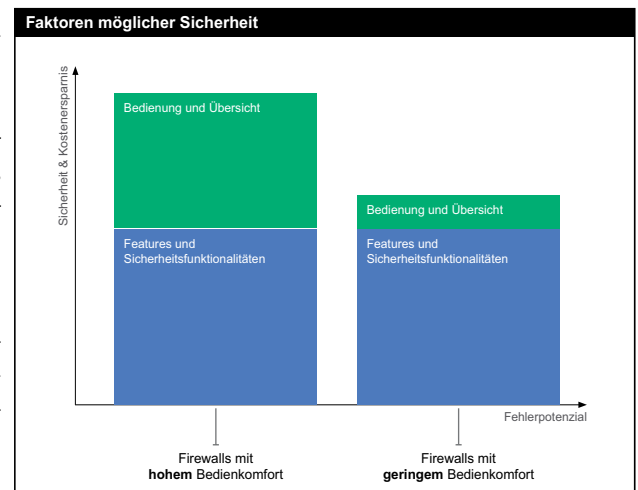
gen der Einstellungen müssten sich dann per Auswahlménú vornehmen lassen.

### Ein gelungener Dialog ist selbstbeschreibungsfähig

Eine Oberfläche, die das Kriterium der „Selbstbeschreibungsfähigkeit“ erfüllt, sollte bei der Wahl der Symbole ein Maß an Informationsgehalt erreichen, das deren Bedeutung möglichst einfach und gleichzeitig eindeutig erkennen lässt. Das Symbol für einen Arbeitsplatzrechner sollte deshalb seinem realen Gegenstück so weit wie möglich ähneln. Andererseits kann man bei der Darstellung eines konkreten Anwenders auf eine grafische Symbolisierung verzichten und einfach dessen Vor- und Zunamen verwenden, um Verwechslungen auszuschließen. Selbstbeschreibungsfähigkeit bedeutet darüber hinaus, dass sich die Bedeutung eines Symbols nicht ändert, unabhängig vom Kontext, in dem es verwendet wird. Kontextabhängige Bedeutungsunterschiede verlangen dementsprechend nach neuen Symbolisierungen, um die Eindeutigkeit zu erhalten.

### Die Steuerung eines Dialogs muss beim Anwender liegen

Um das obige Beispiel wieder aufzugreifen: Die Sicherheitseinstellungen für einen Vertriebsleiter können von denen eines Vertriebsmitarbeiters so deutlich abweichen, dass es einen Umweg und Mehraufwand bedeuten würde, dem Manager zunächst alle Sicherheitseinstellungen der Abteilung



**Gut bedienbare Firewalls erhöhen das Sicherheitsniveau beträchtlich**  
Quelle: Gateprotect

zuzuordnen. Für diesen Fall muss die Administrationskonsole die Möglichkeit bieten, die nötigen Konfigurationen direkt auf der Ebene des Users einzugeben.

### Von besonderer Bedeutung ist das Kriterium der Erwartungskonformität

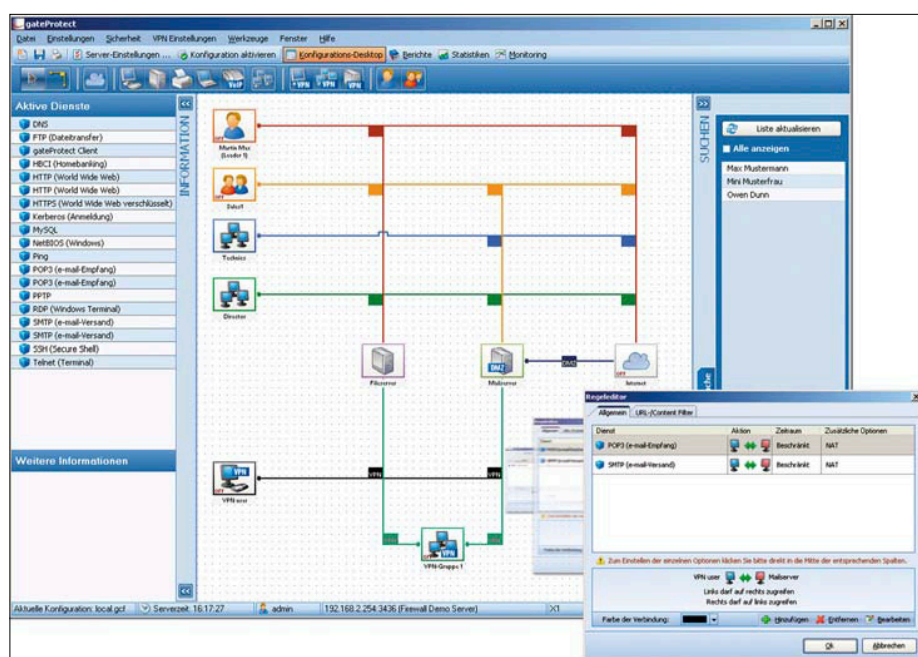
Es ist für einen Anwender unerträglich, wenn innerhalb ein und derselben Anwendungsumgebung Informationen auf unterschiedliche Art und Weise dargestellt werden oder wenn sich das Dialogverhalten und der Dialogwortschatz beim Wechseln von einer in die andere Anwendung ändern. So gehören für den Anwender zum Beispiel URL- und Content-Filtering wie zwei Seiten derselben Medaille zusammen, wenn in diesem Bereich Einstellungen auf Gruppen- oder User-Ebene anzuzeigen sind. Natürlich wirken im Hintergrund zwei verschiedene Firewall-Applikationen, aber die entsprechenden Auswahlmensüs und Konfigurationsmöglichkeiten sind in einer konsolidierten Darstellung zusammenzufassen. Mehr noch: Auch die Nomenklatur beider Anwendungen müssen angeglichen werden. Sollen etwa sexuelle Inhalte und Internetadressen, die auf entsprechende Seiten hinführen, geblockt werden, so müssen die Rubriken sowohl der URLs als auch der Inhalte die gleiche Bezeichnung tragen. Diese Forderung ist nicht trivial, denn gerade in diesem Bereich kommen vielfach OEM-Produkte verschiedener Hersteller zum Einsatz. URL- und Content-Filtering ist übrigens ein hervorragendes Beispiel für das Zusammenspiel aller bisher genannten Kriterien: Eine eindeutige und allgemeinverständliche Nomenklatur eröffnet die Möglichkeit, die Konfiguration auch durch andere Anwender als den IT-Administrator vornehmen zu lassen. Es mag nämlich durchaus Websites geben, deren Domain-Name die Buchstabenfolge „sex“ enthält und die daher geblockt werden, obwohl sie für den Vertrieb wichtig sind. Wer aber kennt diese Websites besser als der Vertrieb? Können die Einstellungen für URL- und Content-Filtering in einem einzigen Dialogfeld von einem Nichttechniker für alle Nutzer der Gruppe „Vertrieb“ vorgenommen werden, dann ist die Benutzerführung aufgabenangemessen, selbst-

beschreibungsfähig und steuerbar, weil den Kenntnissen des Anwenders angepasst.

### Das Benutzerkonzept von Firewalls muss sich durch Lernförderlichkeit auszeichnen

Die Forderung nach „Lernförderlichkeit“ besagt, dass das Maß an technischem Wissen bei der Administration so gering wie

zeigt nach rechts, und dort ist das Internet-symbol platziert. Zur Erklärung muss ein Mausclick reichen, um eine nähere Beschreibung einzublenden. Statt des technischen Begriffs „Stateful Inspection“ reicht dem Nichttechniker eine selbsterklärende Beschreibung völlig aus, etwa: „links darf auf rechts zugreifen, rechts darf nur antworten“. Mehr noch: Gerade durch sol-



Das Design der Benutzerschnittstelle erfordert viel Feingefühl

Quelle: Gateprotect

möglich gehalten werden sollte. So haben Filialen von Einzelhandelsketten oder Banken, geografisch verteilte Produktions- und Vertriebsstandorte großer Unternehmen, aber auch kleinere Unternehmen, die wie Anwaltskanzleien oder Steuerberaterbüros einer besonderen Haftung beim Umgang mit persönlichen Daten unterliegen, ähnlich hohe Sicherheitsanforderungen wie Konzernzentralen, verfügen aber nicht über das gleiche technische Know-how. Daher ist es ratsam, Sicherheitsfunktionen – wo immer möglich – ohne technische Begrifflichkeiten zu beschreiben. Einem im Umgang mit dem Internet geübten Anwender ist zum Beispiel klar, dass die Zugriffsmöglichkeit aus dem Internet auf einen Rechner im eigenen Netz eine große Gefahrenquelle darstellt. In einer grafischen Bedieneroberfläche kann diese Beziehung durch ein Pfeilsymbol dargestellt werden: Links vom Pfeil ist der Rechner dargestellt, der Pfeil

che Formulierungen sinkt das Risiko fehlerhafter Eingaben.

### Fazit

Das ergonomische Design von Firewall-Cockpits schafft einen direkten Zugang zu den verschiedenen Administrationsaufgaben und vermeidet Fehlerquellen durch anwendungsübergreifende Sichten und Steuerungsmöglichkeiten. So wird auch das Delegieren von Administrationsaufgaben an unterschiedliche Benutzergruppen möglich. Dies spart Zeit und Geld und erhöht ganz nebenbei das Sicherheitsniveau – denn erst das Cockpit macht aus guten Autofahrern Formel-1-Piloten.