Professionelle Antiviren- und Contentsecurity für Check Point FW-1™:

Dank des Internets können Sie heute schnell über weite Distanzen Informationen einholen und kommunizieren. Diese enge Vernetzung bringt aber auch immer stärker werdende Gefahren mit sich:

- Computerviren zerstören Ihre Arbeit,
- Mitbewerber interessieren sich mit Hilfe von Trojanern für Ihre Betriebsgeheimnisse,
- Zudem bedrohen Emailviren die Zuverlässigkeit Ihrer Kommunikationsstrukturen.
- Zukünftig wird es noch viele andere elektronische Bedrohungen geben, die Ihnen das Leben schwer machen wollen.

Innovative Scantechnologie:

Die IKARUS ContentWall / CVP scannt und entfernt Emailviren, Makroviren, Würmer, Trojaner, Active Code, Malware, Dialer etc. und verwendet dabei mehrere Methoden:

- Pattern Scanning (für bereits aufgetretene Viren)
- Heuristisches Scanning (für noch unbekannte Viren)
- Heuristisches Scriptscannen (für noch unbekannte Scriptviren)

IKARUS Software war weltweit der erste Entwickler von Antivirenprogrammen (1986). Seit dieser Zeit stehen wir in ständigem Kontakt mit anderen Herstellern und Institutionen, um gegenseitig neue Computerviren auszutauschen. Diese Netzwerke stellen sicher, dass wir Sie in kürzester Zeit vor neuen Bedrohungen schützen können.

Protokolle: HTTP, FTP, SMTP, POP3, IMAP, NNTP:

In der Praxis hat sich gezeigt, dass nicht nur Protokolle wie SMTP, FTP und HTTP in einem Unternehmen verwendet werden, sondern auch IMAP, POP3 und NNTP. Mit der IKARUS ContentWall / CVP können Sie auch diese Protokolle auf Computerviren in Echtzeit untersuchen. Nicht nur das - jedes einzelne Protokoll kann mit spezifischen Settings konfiguriert werden.

Reglementierung des Zugangs zu Newsgroups:

Durch die Fähigkeit auch NNTP zu scannen, können Sie mit der IKARUS ContentWall / CVP den Zugang zu Newsgroups für verschiedene Benutzergruppen individuell reglementieren.

Einfache Anpassung an verschiedene Benutzergruppen:

In jedem Unternehmen gibt es verschiedene Gruppen mit unterschiedlichen Bedürfnissen. So müssen z.B. für einige Benutzergruppen strengere Regeln definiert werden, als für andere. Damit Sie diese Policies einfach und rasch umsetzen können, bietet Ihnen die IKARUS ContentWall / CVP als einzige CVP Lösung die Option der VIRTUELLEN CVP und UFP Server.

CONVERTER - proaktive Emailsecurity:

Der CONVERTER ermöglicht es, alle aktiven Inhalte einer Email zu entfernen. Diese aktiven Inhalte werden von Viren oft als Medium zur Verbreitung ausgenutzt. Mit deren Entfernung entzieht man den meisten Emailviren schon im Vorfeld die Grundlage. Sie selbst können definieren, welche gefährlichen Teile aus den eingehenden Emails gelöscht werden soll. (z.B. vb-scripts, java-scripts, html-tags, iframes, etc.) Dieses Feature erhöht drastisch die Sicherheit vor neuen und unbekannten Fastinfektoren.

OPSEC zertifiziert:

Die IKARUS ContentWall / CVP ist OPSEC-NG zertifiziert. Diese Zertifizierung garantiert dem Endanwender eine einfache Integration in die CVP Umgebung der Check Point FW-1™ .

Effektives URL-Filtering:

Optional bietet Ihnen die IKARUS ContentWall / CVP auch die Möglichkeit des URL-Filterings. IKARUS Software arbeitet in diesem Bereich mit den weltweiten Technologieführern zusammen. Verschiedenste Themengruppen können ausgewählt werden, um Ihre unterschiedlichen Benutzergruppen vor ungeeigneten Inhalten zu schützen.

SPAM-Filter:

Die IKARUS ContentWall / CVP bietet Ihnen die Möglichkeit äußerst effektiv SPAM auszufiltern. Mittels verschiedenster Methoden und selbstlernenden Algorithmen werden Emails nach vielen Regeln bewertet. SPAMs werden erkannt und nach ihrer Konfiguration weiterverarbeitet (löschen, markieren oder redirekten). Die Sensibilität des Spamfilters kann von low bis high in 9 Unterstufen von Ihnen geändert werden. Zusätzlich können Sie selbst Regeln und deren Sensibilität definieren, mit der Sie die Suche nach SPAM verfeinern können. SPAM wird mit der IKARUS ContentWall / CVP mit bis zu 98%er Effektivität ausgefiltert!

Verwendete Technologien:

- Heuristische Analyse
- Bayes'sche Analyse
- Lexikalische Analyse
- Spamdatenbank
- Black- und Whitelists
- Subject Analyse
- Directory Harvesting Protection
- Mailbombing Protection
- Relay Spoofing Protection

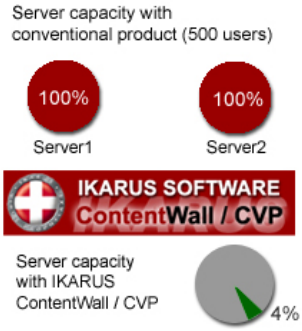
Eine genaue Beschreibung der Technologien und wie sie funktionieren finden Sie in unserem Folder „Antispam Technologien“ oder auf unserer Homepage: www.myspamwall.at

CONTENT-Filter:

Damit keine vertraulichen Informationen nach außen gelangen, ermöglicht Ihnen die IKARUS ContentWall / CVP eine inhaltssensitive Analyse von Emails und deren Attachments. Durch die Definition von Keywörtern kann der Verlust von Unternehmensgeheimnissen verhindert werden. Zugleich werden auch verschlüsselte Emails erkannt, und je nach Konfiguration weiterverarbeitet (gelöscht, in Quarantäne verschoben oder redirektet).

Unschlagbare PERFORMANCE:

Bisher war es nicht möglich Datenmengen von mehr als 250 Usern zuverlässig über CVP zu scannen.
Mit IKARUS ContentWall / CVP gibt es diese Einschränkung nicht mehr. D.h. auch große Datenmengen von tausenden Usern sind kein Problem mehr.



Feature List:

IKARUS ContentWall / CVP

- → **Scannt** HTTP, FTP, SMTP, NNTP, IMAP, POP3
- → **Scannt** und **entfernt** Emailviren, Makroviren, Würmer, Trojaner, Java Applets, Dialer, etc.
- → **Verwendet** 3 verschiedene Scantechnologien.(Schutz vor bekannten und unbekannten Viren)
- → **Managt** den Zugriff auf Newsgroups für verschiedene Benutzergruppen
- → **Filtert** IMAP-, NNTP-, POP3 - Useraccounts und Paßwörter aus dem Traffic
- → **Alarmiert** verschiedene Administratoren per Email
- → **Unterstützt** 17 verschiedene Packalgorithmen
- → **Löscht** aktive Inhalte aus Emails (iframes, etc.)
- → **Managt** die Antivirus-Policies für verschiedene Benutzergruppen (virtuelle CVP und UFP Server)
- → **Filtert** unerwünschte Attachments und Downloads aus dem Datenverkehr mit Hilfe von CONTENTTYPE BLOCKING
- → **Filtert SPAM** mithilfe verschiedenster Methoden
- → **Filtert** verschlüsselte Dateien aus dem Traffic
- → **Updatet** die Virendatenbanken automatisch
- → **Ermöglicht** Rechtevergabe für verschiedene Administratoren
- → **Protokolliert** alle wichtigen Ereignisse (auch direkt in die Check Point Firewall-1™)
- → **Verfügt** über Realtime monitoring zur Überwachung aller Protokolle und Benutzergruppen
- → **IST** Cluster- und loadbalancingfähig

Leistungsfähige Hardware:

Technische Daten:

Die IKARUS ContentWall / CVP verwendet den Scanner IKARUS T2 der als einziger Scanner echtes Multithreading einsetzt.

Ebenso wird Multiprocessing unterstützt, das Ihnen als Benutzer garantiert, dass auch alle zur Verfügung stehenden Prozessoren verwendet werden.

Das System setzt auf einem gehärteten Linux auf, um Stabilität, Performance und Applikationssicherheit garantieren zu können.

Die IKARUS ContentWall / CVP wurde als Hardwaresolution konzipiert um Installationsupport zu vermeiden und die Performance zu optimieren. Die verschiedene Leistungsstufen der SecureGuard Appliances machen das System optimal skalierbar.

IKARUS SOFTWARE

IKARUS Software Deutschland
- VC Europe GmbH -
Münsterstr. 5
D-59065 Hamm
Tel.: (+49) 02381 – 688-580
Fax: (+49) 02381 – 688-455
info@vc-europe.com
http://www.ikarus-software.de