

Der vollständige Bericht ist bei der Zeitschrift FACTS erhältlich.

**Zeitschrift FACTS, Testurteil gut für Securepoint UTM-Lösungen:**



Cyberkriminelle bedienen sich immer raffinierterer Methoden, um in Firmennetze einzudringen, Computer nach brauchbaren Daten zu durchsuchen und schwere wirtschaftliche Schäden zu verursachen. Mit einer professionellen Firewall-Lösung können Unternehmen Datendiebe und Vandalen schon an der digitalen Haustür abfangen. FACTS machte sich anhand einer Ausschreibung auf die Suche nach der geeigneten Lösung für mittelständische Unternehmen.

**D**er Hightech-Verband BITKOM und das Bundeskriminalamt (BKA) haben in einer aktuellen Veröffentlichung vor einer weiteren Professionalisierung von Betrugsmethoden gewarnt. „Schadprogramme sind zunehmend schwerer zu erkennen. Angriffe erfolgen vermehrt über Anwendungsprogramme, und nicht nur über Lücken in Betriebssystemen“, lautet dabei das Fazit von BITKOM.

### SCHADPROGRAMME

Viren und andere Schadprogramme bilden die häufigste Erfahrung mit Online-Kriminalität. Rund 43 Prozent der Internetnut-



# Der Wächter am Tor

zer – das entspricht 22 Millionen Deutschen – haben schon einmal erlebt, dass ihr Computer infiziert wurde. Im Vorjahr waren es noch 38 Prozent. Das geht aus Erhebungen von Forsa für BITKOM hervor. Schadprogramme können nicht nur Rechner lahmlegen, sondern spähen vermehrt auch Daten und Identitäten aus. Für einen zuverlässigen Schutz sorgt eine Firewall, die verdächtige Daten sperrt, bevor diese ins firmeninterne Netzwerk gelangen können.

Im professionellen Umfeld wie in einem Firmennetzwerk ist der Einsatz einer hardwarebasierten Firewall unbedingt zu empfehlen. Gerade wenn in einem Netzwerk vertrauliche Daten und Kundeninformationen abgelegt sind, ist eine professionelle Absicherung unerlässlich. Die Firewall dient da-

zu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Die Firewall überwacht den durch sie hindurchlaufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht die Firewall, unerlaubte Netzwerkzugriffe zu unterbinden.

## PAKETKONTROLLE

Die wohl grundlegendste Funktion einer jeden Hardware-Firewall ist die sogenannte „Stateful Packet Inspection“ (SPI). Dabei wird jedes eingehende Datenpaket einer genauen Prüfung auf Unbedenklichkeit unterzogen, bevor es an die dahinter geschalte-

ten Rechnernetze weitergeleitet wird. Verdächtige Datenströme werden dabei gefiltert, dokumentiert oder ganz blockiert. Datenpakete dürfen auch nur dann passieren, wenn sie in einer aktiven Sitzung (Session) einer laufenden Applikation im Rechnernetz zuzuordnen sind. Damit wird verhindert, dass Daten den Weg ins interne Rechnernetz finden, die von keiner Anwendung angefordert wurden.

Eine SPI alleine kann aber als Schutz nicht ausreichen: Ist ein hinter der Firewall betriebener Rechner beispielsweise mit einem Trojaner infiziert, lässt sich die SPI unter Umständen täuschen, da der Rechner durch den Trojaner bestimmte Daten in der Tat angefordert hat und somit eine gültige Session besteht. ➤