

# SONDERDRUCK für PSP

IM TEST: WALL BOTZ 500 VON NET BOTZ

## Aus der Ferne überwacht

Net Botz bietet mir der Linux-basierten Appliance Wall Botz 500 ein Werkzeug zum Überwachen der Umweltbedingungen in Rechenzentren. Das Produkt ist eine Stand-alone-Lösung, der Hersteller hat jedoch auch Versionen für den Rack-Einbau im Angebot. LANline hat sich die Appliance näher angesehen.

Die Wall Botz 500 ist eine Linux-Appliance auf Power-PC-Basis. Administratoren sind dazu in der Lage, direkt an das Gerät eine Kamera und ein so genanntes Sensor Pod anzudocken. Die Kamera überträgt nicht nur Bilder sondern kann auch über ein angeschlossenes Mikrofon Töne aufnehmen, über Boxen akustische Signale ausgeben und mit einem Türsensor kombiniert werden. An die Appliance lassen sich über USB weitere Kameras anschließen, beispielsweise um andere Bereiche des Rechenzentrums zu überwachen. Unsere Teststellung kam mit zwei Kameras und zwei Sensor Pods, die ihrerseits einen Temperaturfühler, einen Sensor für die Luftfeuchtigkeit,

einen Sensor für den Air Flow sowie einen Sensor für den Dew Point (Taufpunkt) umfassen. Zusätzlich bieten die Sensor Pods noch vier Anschlüsse für externe Sensoren. So lieferte uns Net Botz etwa einen Flüssigkeitsdetektor und einen externen Temperaturfühler, den man beispielsweise in ein Rack hängen kann. Das System unterstützt darüber hinaus auch den Anschluss externer Geräte über ein zweipoliges Kabel. Das ist etwa für Drittanbieterkomponenten sinnvoll, die sich auf diese Weise steuern lassen. Soll die Wall Botz an einem Ort zum Einsatz kommen, der nicht über ein LAN-Kabel erreichbar ist, lässt sich zur Kommunikation mit dem Gerät auch eine Orinoco-kompa-

tible Funk-LAN-Karte in dem extra dafür vorgesehenen PCMCIA-Slot nutzen.

**INBETRIEBNAHME** Nach dem Anschluss aller Sensoren und dem Hochfahren der Appliance hat der Administrator zwei Möglichkeiten, auf die Lösung zuzugreifen. Befindet sich ein DHCP-Server im Netz, besorgt sich die Wall Botz dort direkt eine IP-Adresse, steht kein DHCP-Server zur Verfügung, bietet der Hersteller eine Konfigurationssoftware, die die Netzwerkparameter über den seriellen Port einstellen kann. Um mit dieser Software auf die Appliance zuzugreifen, ist das Root-Passwort erforderlich, das vom Hersteller im Quick-Start-Guide angegeben wurde. Etwas verwirrend: Spätere Zugriffe auf das Produkt über das Webinterface und die Administrationssoftware laufen dann nicht über das gleiche Konto, sondern über einen anderen Benutzer namens netbotz. Wir scheiterten nach der Netzwerkkonfiguration deshalb mit unseren Zugriffsversuchen – die Hinweis auf den netbotz-Anwender fand sich nämlich erst nach einigem suchen im Handbuch (das übrigens als PDF-Datei auf CD vorliegt). Was die Netzwerkkonfiguration angeht, ist noch wichtig zu erwähnen, dass das dafür

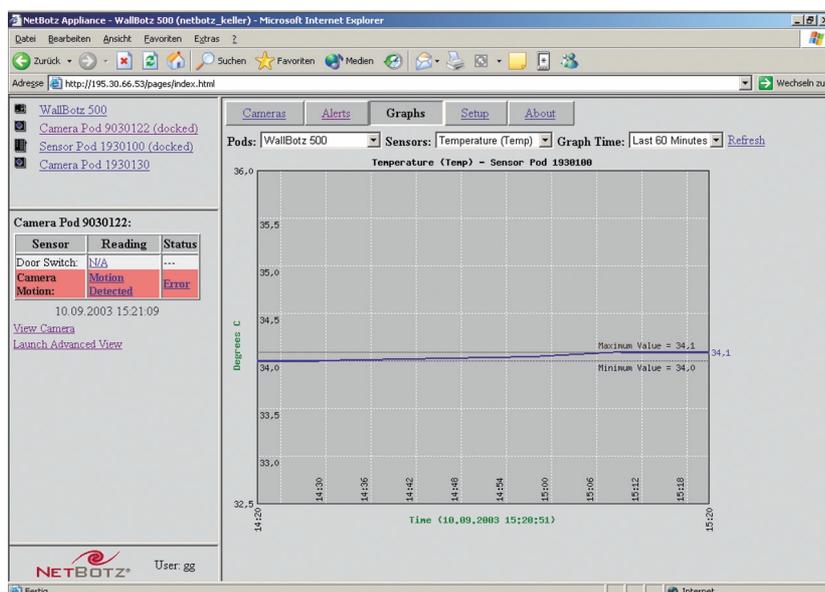
vorgesehene Tool sowohl das LAN-Interface als auch die WLAN-Karte konfigurieren kann, bei WLANs fiel jedoch auf, dass sich lediglich ein WEP-Key für die Verschlüsselung speichern lässt und nicht, wie normalerweise üblich, mehrere.

Sowohl das Netzwerkkonfigurationswerkzeug als auch die Viewer/Administratorsoftware basieren auf Java, und der Hersteller bietet Viewer für Windows- und Linux-Clients an. Im Test kamen ein Windows 2000 Server mit Service-Pack 4 und ein Debian 3.0 System zum Einsatz, und die Software funktionierte in beiden Fällen identisch.

**ADMINISTRATION** Nach der Vergabe der Netzwerkparameter wie IP-Adresse, Subnetzmaske, Gateway und Ähnlichem erfolgt der weitere Zugriff auf die Appliance über einen Web-Browser oder die mitgelieferte Advanced View Software. Das Browser-Interface genügt, um die aktuell gemessenen Werte einzusehen und die Bilder der Kameras darzustellen, zur Konfiguration der Lösung muss jedoch Advanced View zum Einsatz kommen. Damit Administratoren von allen Arbeitsstationen aus problemlos auf diese Software zugreifen können, findet sich auf der Website der Appliance ein Download-Link zum Hersteller. Der Download wird seltsamerweise über ein Java-Applet gesteuert. Unter Windows treten dabei keine Probleme auf, unter Linux kommt es aber zu der grotesken Situation, dass man auf seinem Linux-Rechner eine funktionierende Java-Umgebung einrichten muss, nur damit der Download einer Software funktioniert, die ihrerseits eine komplette Java-Virtual-Machine für Linux mitbringt. Hier wäre ein direkter Link wünschenswerter gewesen.

Hat man Advanced View erst einmal installiert, stehen umfangreiche Konfigurationsmöglichkeiten zur Verfügung. Wer Wert auf Sicherheit legt, kann beispielsweise eine Verschlüsselung der Zugriffe über SSL erzwingen. Neben Angaben zu Log-Level und Syslog-Host ist der Administrator an dieser Stelle zudem in der Lage, einen E-Mail-Server zu definieren, über den Mail-Benachrichti-

Konfigurationsbereich der Appliance ab. Hier können die Verantwortlichen verschiedene Benutzer mit unterschiedlichen Rechten definieren, beispielsweise welche die die Lösung administrieren dürfen und andere, die lediglich Zugriff auf die Anwendung haben. Im Test kam es dabei allerdings zu erheblichen Schwierigkeiten. Beim Speichern unserer Änderungen an der Benutzerkonfiguration



Übersichtlich: Die grafische Darstellung der Messwerte

gungen herausgehen. Zusätzlich kann er die Zeitzone setzen, einen SNMP-Agenten aktivieren und ein Upgrade der Firmware beziehungsweise des Advanced Viewers durchführen. Letzteres funktioniert hervorragend: Direkt aus dem Upgrade-Dialog heraus sucht die Appliance auf der Website des Herstellers nach den aktuellen Versionen und lädt sie auf Wunsch herunter um sie automatisch zu installieren. Es ist also nicht erforderlich, die Net-Botz-Download-Site zu durchsuchen und das Firmware-Image manuell auf die Appliance hochzuladen. Ein Dialog zum Anlegen von Benutzern schließt den

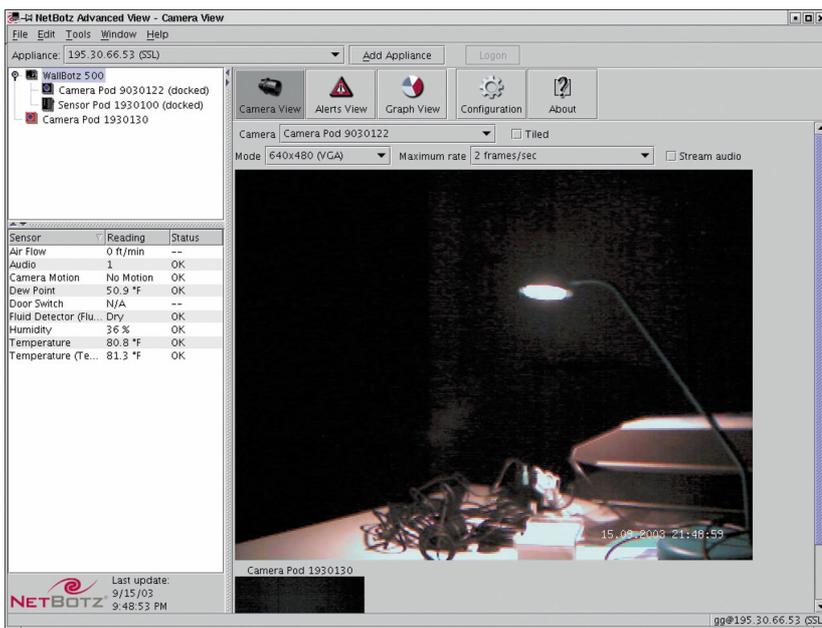
meldete die Appliance, dass sie nicht in der Lage sei, den Benutzer "netbotz" abzuspeichern und verabschiedete sich anschließend. Es war danach nicht mehr möglich, sich auf dem Produkt einzuloggen – egal mit welchem Konto wir es versuchten. Folglich stand ein Factory Reset an. Leider fand sich nirgendwo in der Dokumentation ein Hinweis wie dieser zu bewerkstelligen sei. Hier bewährte sich der Support des Herstellers, der innerhalb weniger Stunden eine Anleitung zum Factory Reset bereitstellte: Verbinden eines Clients über serielles Kabel, Aufbau einer Terminal-Session mit den Parametern

38.400 Bits/s, 8 Datenbits, keiner Parität, einem Stopbit und Hardwareflusssteuerung. Bootet man nun die Appliance und stoppt den Autoboot-Prozess durch einen Tastendruck, landet man auf einer Kommandozeile. Der Befehl "configreset" setzt die Lösung nun zurück. Daraufhin konnte die Konfiguration bei uns wieder von

ner "program files" findet. Anschließend stehen umfangreiche Erklärungen zur Verfügung, und die weitere Einrichtung des Systems verläuft unproblematisch. Das Produkt bietet mehrere verschiedenen Benachrichtigungsmöglichkeiten: E-Mail, FTP, SNMP oder HTTP-Post. Die Lösung ist zudem in der Lage, über an die Ka-

richtigende Adressen zuweisen, das heißt, bestimmt Alarme gehen auch an die dafür verantwortlichen Personen. Außerdem bietet das Werkzeug noch Optionen zum Einstellen von Parametern wie Helligkeit und Frame-Rate.

"Alert Profiles" dient zur genaueren Definition der Alarme. So gibt es ständige Alarme und unterschiedliche Alarm-Level, auf denen sich den einzelnen Alerts wiederum unterschiedliche Aktionen zuordnen lassen. Der Punkt "Periodic Reports" wiederum ermöglicht das Konfigurieren regelmäßiger Reports. Das System unterstützt E-Mail-, FTP- oder HTTP-Reports. Diese Reports können bei Bedarf auch die Bilder der Kameras mit einschließen.



Advanced View sieht unter Linux genauso aus wie unter Windows

vorne beginnen. Bei dem zweiten Versuch gab es dann auch keine Probleme mit der Änderung der Benutzerkonten.

**IM EINSATZ** Nach dem glücklichen Überwinden sämtlicher Konfigurationshürden, machten wir uns an die Überwachung unseres Rechnerraums. Möchte ein Administrator, der mit einem deutschen Windows arbeitet, die Hilfefunktion der Appliance nutzen, muss er zunächst im Advanced Viewer unter Edit/Preferences/General den Pfad zum Browser anpassen, da dieser sich auf deutschen Systemen bekanntermaßen im Ordner "programme" und nicht im Ord-

ner "programme" befindet. Die Kamera angeschlossene Boxen Audio-Alerts auszugeben.

Der Punkt "Sensor Pod" ermöglicht es dem Verantwortlichen, eigene Sensoren zu definieren und dem System mitzuteilen, welche Sensoren an den externen Anschlüsse arbeiten (in unserem Fall ein zusätzlicher Temperaturfühler und der "Fluid Detector"). Unter "Sensors" kann er dann den Sensoren Grenzwerte zuweisen, deren Überschreitung einen Alarm auslöst. Der Punkt "Camera Pods" dient wiederum zum Aktivieren eines Bewegungsalarms und zur Konfiguration der Türsensoren. Administratoren können übrigens allen Grenzwerten bestimmte zu benach-

**IM TEST** Bei der täglichen Arbeit liefert das Produkt übersichtliche und leicht verständliche Informationen zu allen überwachten Parametern. Sowohl Advanced View als auch das Webinterface zeigen links oben die angeschlossenen Pods und darunter die jeweils entsprechenden Statusmeldungen. Unter "Camera View" lassen sich die Bilder der Kameras anzeigen, entweder mit einem großen und einem kleinen Bild, oder alle Bilder in gleicher Größe nebeneinander. Hier kann der Administrator auch die Frame-Rate einstellen und den Ton des gerade an die aktive Kamera angeschlossenen Mikrofons wiedergeben. "Alerts View" zeigt im Gegensatz dazu eine Liste der aufgelaufenen Alarme, während "Graph View" diese grafisch aufbereitet. Insgesamt hinterlässt der in der Grundausstattung 3000 Euro teure Web Botz 500 einen guten Eindruck, denn sobald das System einmal läuft, liefert es zuverlässig alle vom Administrator gewünschten Informationen.

(Götz Güttich)