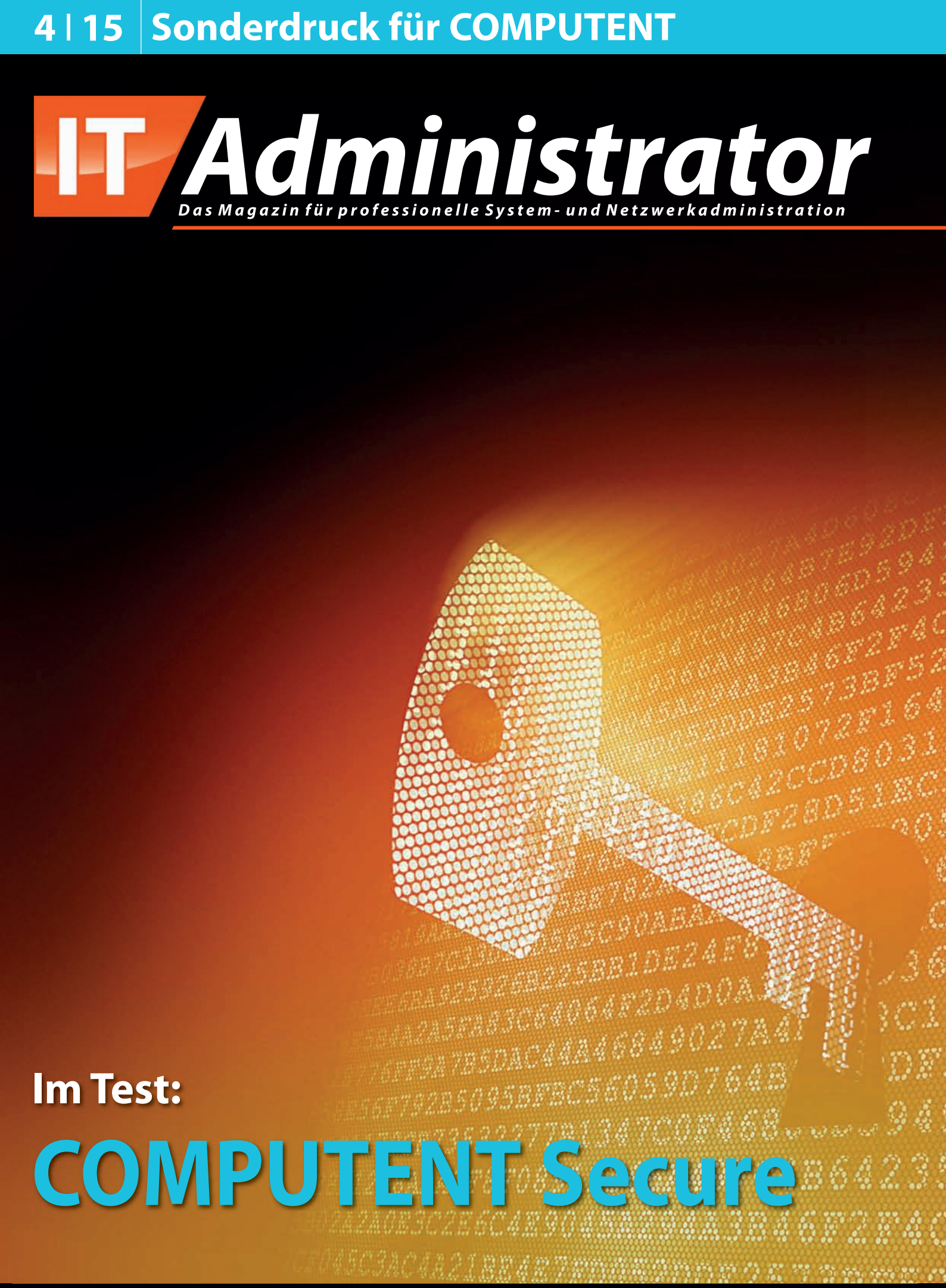
4 | 15 Sonderdruck für COMPUTENT

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration



Im Test:

COMPUTENT Secure

www.it-administrator.de

Im Test: COMPUTENT Secure

Fern und doch ganz nah

von Daniel Richey

VPNs für den sicheren Remotezugriff auf lokale Dienste sind eine praktische Angelegenheit und müssen nicht kompliziert sein. Für kleine Umgebungen hat der bayerische Hersteller COMPUTENT die kompakte Secure-Appliance im Angebot. Sie lässt sich mit wenigen Mausklicks einrichten und erlaubt Mitarbeitern den sicheren Zugriff auf lokale Ressourcen per USB-Stick. IT-Administrator hat die Secure-Box ausprobiert.

Eine kleine, unscheinbare Appliance und eine Handvoll USB-Sticks. Diesen Eindruck erweckt die VPN-Lösung COMPUTENT Secure beim Auspacken. Umso überraschter dürfte der Administrator ob der Einsatzmöglichkeiten der VPN-Umgebung sein. Denn das Prinzip, auf dem der sichere Remote-Zugang basiert, ist denkbar simpel: Über die USB-Sticks bauen Mitarbeiter von beliebigen Rechnern aus einen mit 2.048 Bit RSA-verschlüsselten SSH2-Tunnel ins Firmennetzwerk auf und können über diesen beliebige TCP-basierte Anwendungen beziehungsweise deren Daten schleusen. Im internen Netzwerk landen diese Verbindungen in der Secure-Box und werden von dort aus als lokaler Traffic an die Zielserver weitergeleitet – ganz so, als säße der Client im lokalen Netz.

Alles, was der Administrator machen muss, ist die USB-Sticks mit den Zugangsschlüsseln sowie den gewünschten Applikationen zu bestücken. Voreingestellt ist bereits der RDP-Zugriff. Dies ist auch die einzige offiziell unterstützte Anwendung. Alle anderen Applikationen betreibt der Administrator quasi auf eigene Gefahr. Wenig verwunderlich, dass der Hersteller angesichts der denkbaren Vielfalt an möglichen Anwendungen nicht für deren Funktionieren garantieren kann. Auch sind die Anwendungen nicht wirklich vom Gastrechner abgeschirmt und laufen nicht etwa in einem virtuellen Container. Sie starten lediglich vom USB-Stick und nutzen den auf dem Gastrechner aufgebauten SSH-Tunnel ins Firmennetz.

Schnelle Inbetriebnahme

Das Anschließen der Box ist schnell erledigt: Strom- und LAN-Kabel einstecken, fertig. Wo das Gerät im Netzwerk steht, spielt keine Rolle, solange es Kontakt ins Internet hat und die lokalen Server erreicht. Die Verwaltung erfolgt über ein schlicht gehaltenes Webinterface. Hierfür muss der Administrator zunächst einen Rechner in den voreingestellten IP-Adressbereich 192.168.2.x holen und kann anschließend die Netzwerkeinstellungen der Box für die lokale Umgebung konfigurieren. Erreichbar ist die Appliance per HTTP unter ihrer lokalen IP-Adresse. Auf HTTPS-Anfragen reagierte die Appliance in unserem Test zunächst nicht. Hierfür mussten wir den Port 8443 mitgeben, da auf 443 der SSH-Server lauschte. In der ansonsten gut verständlichen Dokumentation fehlte dieser Hinweis.

Das Webinterface ist übersichtlich und funktional aufgebaut. Es gliedert sich in fünf Menüpunkte, die das System, die Netzwerk-Einstellungen, den eigentlichen Secure-Dienst sowie die vorhandenen Lizenzen und weitere Tools betreffen. Die Konfigurationsarbeit beginnt wie erwähnt im Netzwerk-Unterpunkt, wo die lokale IP-Adresse der Box an die Umgebung angepasst wird. Anschließend führt der Weg in den Menüpunkt "Lizenzen". Hier trägt der Administrator die vorhandenen Lizenzschlüssel für die Appliance selbst sowie die einzelnen Nutzer ein.

Damit ist das Gerät bereits betriebsbereit und wartet fortan unter seiner lokalen IP-Adresse auf Port 443 auf SSH-Verbindungen. Unser Augenmerk galt daher als Nächstes der Firewall im Netzwerk, auf der wir eine Portweiterleitung für die SSH-Tunnel einrichteten. Der lokale SSH-Server-Port lässt sich bei Bedarf anpassen, was natürlich in der Portweiterleitung entsprechend berücksichtigt werden muss. Im Bereich "WAN-Netzwerk-Konfiguration" trugen wir nun die externe IP-Adresse unseres Internet-Providers ein sowie den Port, den wir in der Firewall geöffnet hatten. Diese Informationen landen in den Konfigurationsdateien auf den USB-Sticks,

Systemvoraussetzungen

Möglich sind maximal 10 gleichzeitige VPN-Verbindungen, was laut Hersteller etwa einem Datendurchsatz von etwa 4 MBit/s entspricht. Die Client-Applikation arbeitet Java-basiert und setzt Windows als Betriebssystem voraus. Eine lokal installierte Java-Umgebung ist jedoch nicht notwendig. Ob es sich um eine 32- oder 64 Bit-Plattform handelt, hängt von der genutzten Anwendung auf dem USB-Stick ab.

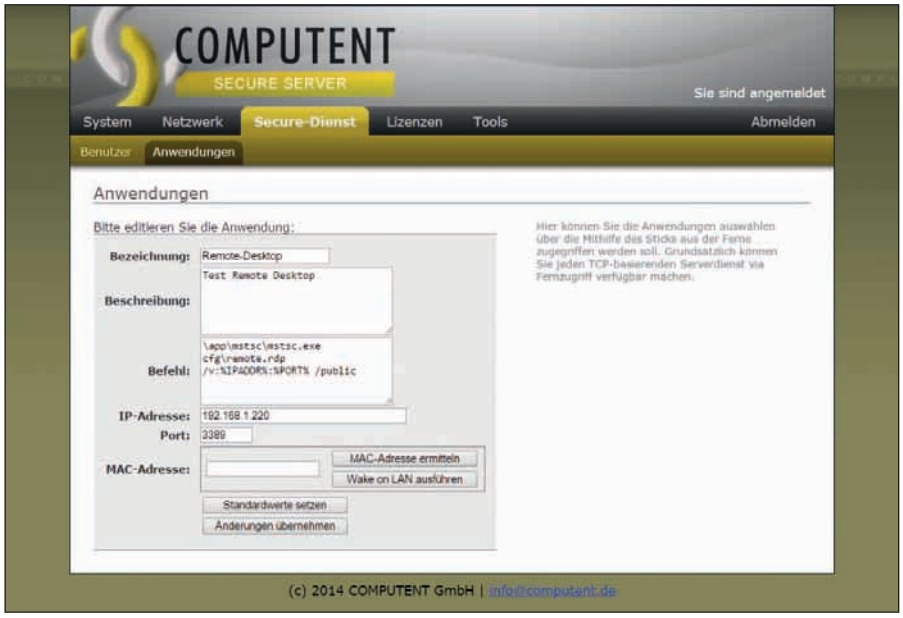


Bild 1: Anwendungen werden über einen Befehl samt Parametern aufgerufen. Praktisch: Für RDP hat der Hersteller bereits alles Nötige eingetragen.

sodass die Clientsoftware unterwegs weiß, wohin sie ihren Tunnel aufbauen soll. Sollte ein Unternehmen nicht über eine statische IP-Adresse verfügen, dann lässt sich auch einfach ein Hostname, zum Beispiel über DynDNS, verwenden.

Nutzer anlegen und Dienste zuweisen

Im nächsten Schritt legten wir die Benutzer an und wiesen den zugehörigen USB-Sticks die grundlegende Konfiguration sowie die vorgesehenen Anwendungen zu. Hierzu später mehr. Für die Userverwaltung dient der Punkt "Secure-Dienst / Benutzer". Zunächst mussten wir die User-Lizenzen eintragen; erst dann ließen sich logischerweise die Benutzer einrichten. Diesen gaben wir einen Anzeigenamen und ein Passwort, das sie bei jedem Start des Clients eingeben. Das Kennwort muss aus mindestens sechs Zeichen bestehen - auf mehr Komplexität bestand die Box in unserem Test nicht. Anwender können ihr Passwort bei Bedarf jederzeit über die Clientsoftware auf dem USB-Stick ändern.

Um den individuellen USB-Stick in der Secure-Appliance aktiv zu schalten, trugen wir nun die Seriennummer des Sticks in das entsprechende Feld ein. Anhand dieser und einer Keycode-Datei identifiziert die Secure-Appliance die USB-Sticks. Auf diesem Weg lassen sich verlorene oder entwendete Sticks sperren. Nachdem unsere Sticks damit aktiv geschaltet waren, wiesen wir die Anwendungen zu. Bis zu 50 lassen sich hierfür in der Box insgesamt hinterlegen. Dabei handelt es sich um einen Befehl, der von der Clientsoftware auf dem USB-Stick ausgeführt wird und eine dort abgelegte Applikation samt Parametern startet.

RDP-Verbindung vorbereitet

Die RDP-Verbindung – der vom Hersteller standardmäßig vorgesehene Verwendungszweck – ist bereits als Anwendung samt Kommando und Parametern hinterlegt. Wir mussten daher nur noch die IP-Adresse mit Portnummer unseres Zielrechners in den entsprechenden Feldern eintragen. Da COMPUTENT aus lizenzrechtlichen Gründen den RDP-Client nicht schon mit den USB-Sticks ausliefern darf, kopierten wir diesen mit einem bereits auf dem Stick vorhandenen Tool von unserem Konfigurationsrechner auf den USB-Stick. Grundsätzlich ist es natürlich sinnvoll, portable Anwendungen auf dem Stick zu nutzen, damit diese auf unterschiedlichen Gastrechnern funktionieren. Schlafende Server lassen sich übrigens per Wake-on-LAN aufwecken.

Um sich vor gravierenden Konfigurationsfehlern zu schützen, bietet die Secure-Box ein Sichern der Einstellungen auf einem externen Speichermedium an. Das kann beispielsweise der Konfigurations-PC sein. So lässt sich im Fehlerfall ein funktionierendes Setup zurückspielen und damit etwa versehentlich gelöschte Einstellungen. Daneben ist ein Reset auf Werkseinstellungen möglich.

Einfache Handhabung für Anwender

Die Pflichten des Administrators sind getan und die Mitarbeiter dürfen sich nun mit ihren freigeschalteten USB-Sticks an Windows-Gastrechnern ins Firmennetz tunneln. Auch hier hat es der Hersteller einfach gehalten: Nach dem Einstecken des Sticks startet der User den VPN-Client, sofern dieser nicht per Autorun ausgeführt wird. Im sich öffnenden Fenster tippt der Nutzer sein zugewiesenes Passwort ein und der Rechner verbindet sich mit der externen IP-Adresse des Unternehmens und weiter ins Firmennetz auf die Secure-Appliance.

Nach der erfolgreichen Authentifizierung des USB-Sticks sieht der Anwender die Bestätigung "Verbindung hergestellt" sowie die ihm zur Verfügung stehenden Applikationen in einer Auswahlliste; in unserem Fall die RDP-Verbindung. Nach einem Klick auf ebendiese startete im Test der lokale RDP-Client, den wir zuvor auf den USB-Stick kopiert hatten, und es erfolgte die Abfrage der RDP-Credentials. Das war's.

Dass COMPUTENT den Fokus auf RDP-Verbindungen gelegt hat, sahen wir auch daran, dass es hierfür ausgiebige Konfigurationsmöglichkeiten in der Clientsoftware gibt. So können Nutzer bestimmen, wie sich das RDP-Fenster öffnen

Bild 2: Das Client-Interface zeigt den Verbindungsstatus.

soll (bestimmte Größe oder Vollbild) und ob ein lokales Laufwerk an den Remote-Rechner für den Datentransfer durchgereicht werden soll. Der funktioniert bei RDP-Sessions nämlich nicht via Copy & Paste oder Drag & Drop. Auch das klappte im Test reibungslos und wir sahen unser lokales Gastrechner-Laufwerk auf dem RDP-Desktop als Netzlaufwerk.

An weiteren Funktionen steht noch ein simples Protokoll zur Verfügung, das jedoch lediglich das Funktionieren oder Nicht-Funktionieren einer Verbindung mit "OK" und "Fehlgeschlagen" wiedergibt. Ferner lassen sich bei Bedarf Proxy-Einstellungen vornehmen, sollte der Gastrechner dies für den Internet-Zugang benötigen.

Einbinden von Drittanwendungen

Als Nächstes versuchten wir unser Glück mit einem portablen FTP-Client. Dieser sollte sich ebenfalls durch den SSH-Tunnel ins lokale Netzwerk verbinden und dort auf einen FTP-Server zugreifen. Wir richteten die Anwendung – also den Aufruf des WinSCP-Clients auf dem USB-Stick – im Webinterface ein und wiesen die Anwendung über den Benutzer-Menüpunkt unserem Teststick zu. Anschließend kopierten wir den portablen Client auf den Stick.

Nach dem Einstöpseln am Gastrechner und der anschließenden Authentifizierung stand der neue Eintrag "WinSCP" als zweite Option neben unserer RDP-Verbindung zur Verfügung. Wir starteten den FTP-Client, der sich öffnete, und versuchten, uns auf den lokalen FTP-Server zu verbinden. Allerdings ignorierte unser FTP-Client den bereitstehenden SSH-Tunnel getrost und wollte sich stets direkt mit der internen IP-Adresse verbinden. Erst als wir über die Variablen "%IPADDR%:%PORT%" die lokale IP-Adresse und den Port des SSH-Tunnels im Programmaufruf mitgaben, loggte sich der Client über den Tunnel erfolgreich auf dem Server ein:

```
WinSCP.exe ftp://Benutzer:Passwort@
  %IPADDR%:%PORT%
```

Es ist stets notwendig, dass die verwendeten Applikationen bei ihrem Aufruf eine lokale, durch die Client-Software vergebene IP-Adresse, die in den SSH-Tunnel führt, als Option mitgeliefert bekommen und akzeptieren. Diese liegt im Adressbereich 127.0.0.x. Auch hierzu wäre ein ergänzender Satz in der Dokumentation sicher hilfreich gewesen.

Mit App und ohne Stick ins Netzwerk

Für mobile Nutzer bietet der Hersteller auch eine App an, die unter Android und iOS läuft. Mit ihr ist der Zugriff auf den RDP-Desktop möglich. Eine transparentgrau hinterlegte Fläche dient als Touchpad, über das sich der Mauszeiger bewegen lässt. Der Administrator hat beim Anlegen des Benutzers die Wahl, ob er diesem einen USB-Stick oder einen SSH-Zugang per App zuweist. Herunterladen können Nutzer oder der Administrator die Apps aus Google Play sowie dem Apple App Store für 7,99 Euro.

Seit Herbst 2014 ermöglicht COMPUTENT den Zugang auch nur per lokal installierter Software. Dies richtet sich an Nutzer, die regelmäßig von einem bestimmten PC aus remote aufs Firmennetz zugreifen möchten, etwa dem Heimrechner. Die Software überprüft dann anhand der Festplatten-ID, ob sie sich auf dem vorgesehenen PC befindet und nicht auf einem unbekannten Rechner gestartet wurde. Damit gilt der gesamte Heim-PC neben dem Passwort als zweiter Faktor bei der Anmeldung. Für noch mehr Sicherheit unterstützt der Hersteller zudem Drittanbieter-USB-Sticks etwa von Kobil, die eine hardwarebasierte PIN-Eingabe ermöglichen. Damit sichert ein weiterer Faktor die Anmeldung ab.

Fazit

Die VPN-Appliance Secure erwies sich im Test als einfach zu konfigurieren: Einstecken, Grundeinstellungen vornehmen, Benutzer einrichten, fertig. Der von COMPUTENT standardmäßig vorgesehene RDP-Zugriff funktionierte auf Anhieb und bietet auch im Client-Interface zahlreiche Optionen. Was die Nutzung anderer Software angeht, muss der Administrator ausprobieren, ob diese mit dem SSH-Tunnel zurechtkommt. Das Webinterface ist simpel und funktional aufgebaut.

Für kleine Unternehmen, die ihren Mitarbeitern einen einfachen wie möglichst sicheren Remotezugriff anbieten möchten, ist COMPUTENT Secure eine interessante Alternative. Es lässt sich auch ohne Fachkenntnisse schnell und einfach in Betrieb nehmen und fügt sich ohne nennenswerten Anpassungsbedarf in eine bestehende IT-Umgebung ein. IT

Produkt
Linux-basierte SSH-VPN-Appliance für kleinere Windows-Umgebungen.

Hersteller
COMPUTENT GmbH
www.computent.de

Preis
Die getestete Ausführung COMPUTENT Secure Pro kostet 480 Euro ohne Nutzerlizenzen. Sie unterstützt bis zu 10 gleichzeitige VPN-Zugriffe. Pro Benutzer kommen nochmal 99 Euro drauf. Die Variante Secure Basic gibt es dagegen für 345 Euro inklusive einer Lizenz; sie unterstützt maximal zwei Benutzer. Ein Upgrade von Basic auf Pro ist ohne Hardware-Tausch möglich.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Sicherheit	7
Konfiguration	7
Client-Usability	8
Flexibilität	7
Skalierbarkeit	6

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für kleinere Umgebungen, in denen eine überschaubare Anzahl an Anwendern von unterwegs per RDP sicher auf Remotedesktops zugreifen möchte.

bedingt für Unternehmen, die neben RDP auch andere Dienste per VPN bereitstellen möchten. Diese werden vom Hersteller offiziell nicht supportet und müssen ihre Tauglichkeit in der Praxis beweisen.

nicht für große Umgebungen sowie Nutzer, die von Linux- oder Mac OS-Rechnern aus eine VPN-Verbindung aufbauen möchten. Es lassen sich nur Windows-Anwendungen nutzen.

COMPUTENT Secure Pro