

Link: <https://www.computerwoche.de/a/sechs-tipps-fuer-ein-effizientes-vpn-gateway,2363553>

Remote Access

## Sechs Tipps für ein effizientes VPN-Gateway

Datum: 02.02.2011  
Autor(en):Ima Buxton

**Teuer, kompliziert und aufwendig, das verbinden viele Unternehmen mit dem Thema Remote-Access. Doch aktuelle Software-Pakete bieten durchaus leistungsfähige und komfortable Lösungen. Lesen Sie, wie Sie die richtige Remote Access Software für Ihr Unternehmen finden - Tipps vom Spezialisten für Fernnetzwerke NCP engineering.**

Das wachsende Heer freier Mitarbeiter und mobiler Arbeitskräfte stellt immer mehr Unternehmen vor die Frage, wie diesen Usern Zugang zu wichtigen Unternehmensdaten gewährt werden kann, ohne dass Aufwand und Risiko für die IT-Abteilungen Überhand nehmen.

Viele Firmen entscheiden sich für den Einsatz eines VPN Gateways und implementieren dafür Software-Pakete, die den effizienten Einsatz von Remote Access nicht ausreichend unterstützen, meint der Spezialist für Fernnetzwerke NCP engineering. Damit Unternehmen bei der Wahl eines Remote-Access-Systems sich nicht von verbreiteten Vorurteilen über Remote-Access leiten lassen, hat der Anbieter NCP engineering jetzt eine Liste mit den wichtigsten Irrtümern über Fernnetzwerke publiziert. Daraus lassen sich für Unternehmen sechs wichtige Tipps für den Erwerb einer VPN-Software ableiten:

[Hinweis auf Bildergalerie: **6 Tipps erfolgreich Remote Access zu nutzen** ] <sup>gal1</sup>

---

### Bildergalerien im Artikel:

<sup>gal1</sup> **6 Tipps erfolgreich Remote Access zu nutzen**



### **Zentrales Management**

Tipp 1: Die Einrichtung von Remote Access bringt ohne Frage einen gewissen Verwaltungsaufwand für den Systemadministratoren mit sich. Dabei müssen Aspekte wie die Einrichtung der VPN-Clients, die Art der Authentifizierung, Endpoint-Security-Check und die Art Zugangs etwa über Mobilfunk oder WLAN berücksichtigt werden. Das klingt kompliziert, ist es aber nicht, meinen die Experten von NCP engineering - sofern eine Lösung zum Einsatz kommt, mit der sich ein Remote Access-Netzwerk über eine zentrale Konsole administrieren lässt. Eine solche VPN Client Suite erlaubt die weitgehend automatische Einrichtung und Betreuung des Fernzugangsnetzwerks.

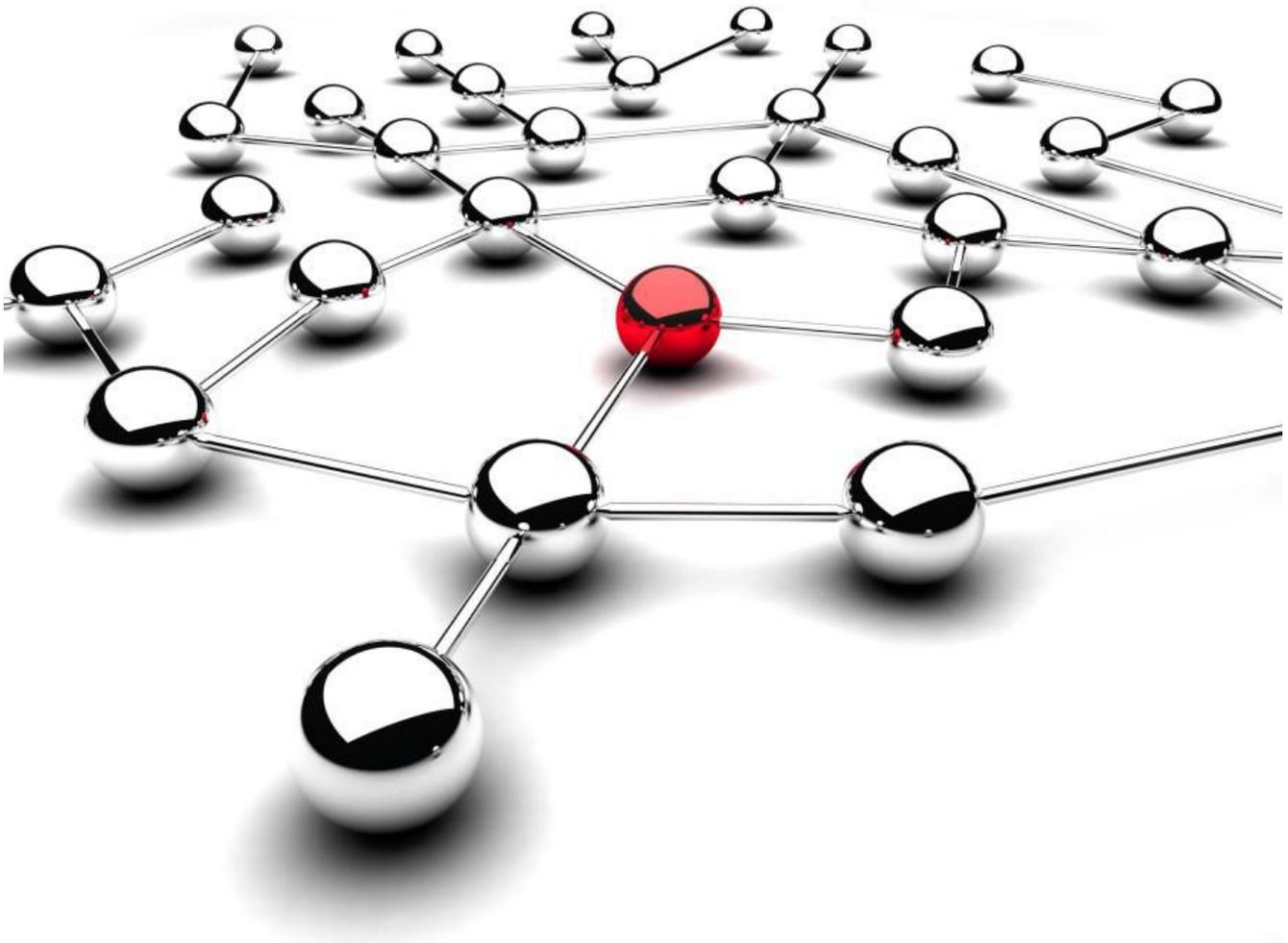
Foto: (c) Phoenixpix\_Fotolia



### **Vorsicht Kostenfalle**

Tipp 2: Zwar sind VPN-Softwarepakete in der Anschaffung relativ günstig, ihre Nutzung zieht jedoch Folgekosten nach sich, die viele Anwender oft übersehen, warnt NCP engineering. Der Betrieb einer Firewall etwa, die Erstellung einer Dokumentation, die Schulung von Nutzern, Updates und vieles mehr können die wahren Kosten einer Remote-Access-Lösung in die Höhe treiben. Um die Kosten in der Produktivphase im Griff zu behalten, empfehlen die Remote-Spezialisten von NCP engineering eine Lösung mit hohem Automatisierungsgrad. Je weniger Klicks End-User und Administratoren benötigen, um eine VPN-Verbindung aufzubauen, um so besser.

Foto: (c) Michael Nivelet\_Fotolia



### **Stabile Verbindung herstellen**

Tipp 3: Viele VPN-Systeme benötigen zahlreiche Klicks zur Herstellung einer Verbindung, die wertvolle Arbeitszeit kostet. Hier kann eine „One-Klick-Lösung“ helfen, bei der der User per Button-Klick eine Software aktiviert, die vom Aufbau der Verbindung bis zur Anpassung der Firewall-Regeln alles regelt.

Tipp 4: WLAN-Hot-Spot sicher nutzen Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

Foto: (c) Phoenixpix\_Fotolia



#### **WLAN-Hot-Spot sicher nutzen**

Tip 4: Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

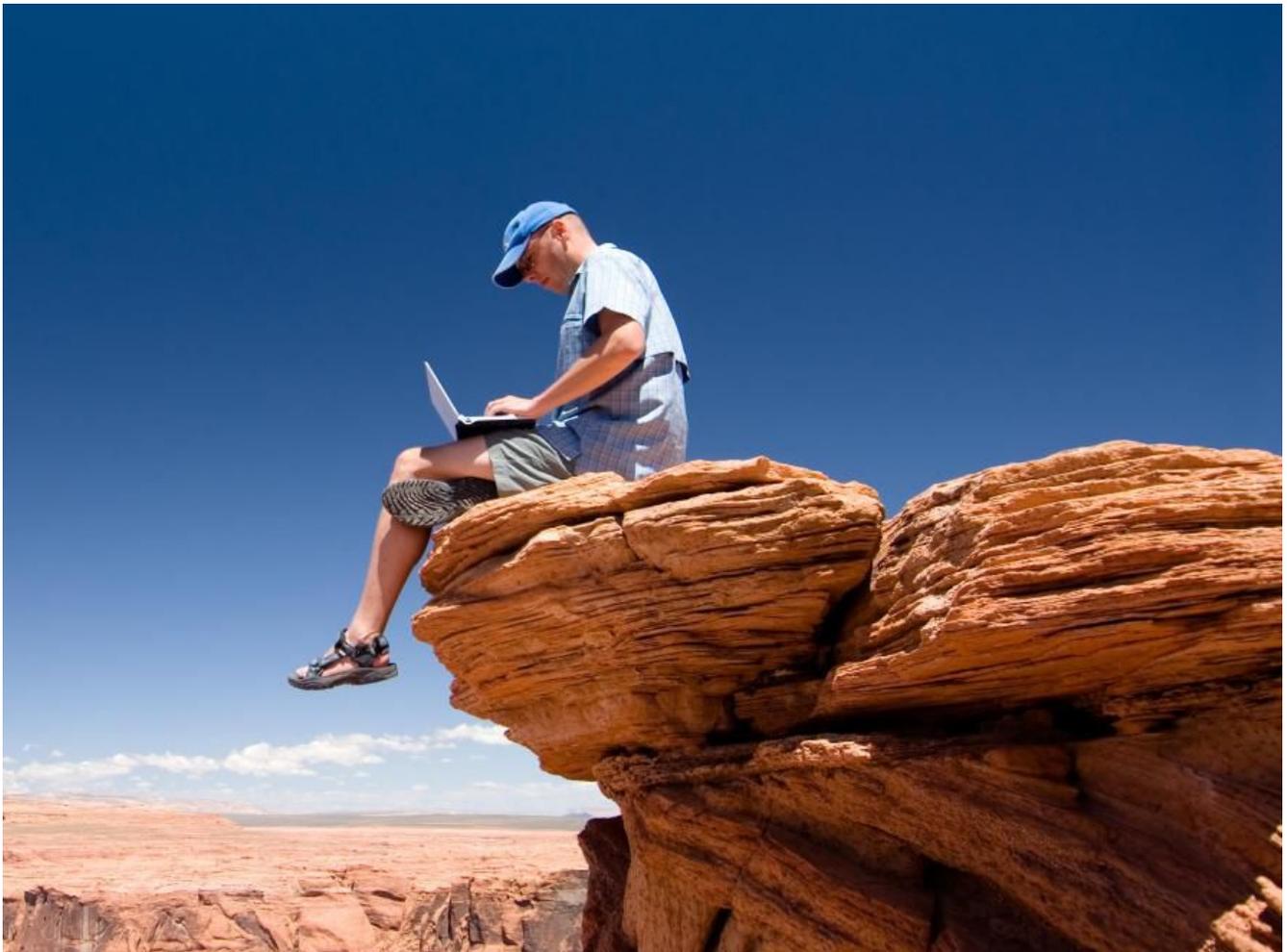
Foto: (c) WoGi\_Fotolia



#### **Kein Zugriff für User auf die Firewall:**

Tipp 5: Anders als von Anwendern vermutet, passen Personal Firewall-Einstellungen eines Client-Systems keineswegs für alle Remote-Access-Szenarien, mahnt NCP engineering. Ob nun öffentlicher WLAN-Hot-Spot oder Firmen-Außenstelle - unterschiedliche Remote-Access-Umgebungen erfordern unterschiedliche Firewall-Regeln. Und diese sollten von IT-Administrator vorgegeben werden, nicht vom User. Das senkt das Risiko von Bedienungsfehlern und das Sicherheitsrisiko.

Foto: (c) imageteam\_Fotolia



### **Automatische Verbindungswahl**

Tipp 6: Viele User nutzen je nach Aufenthaltsort verschiedene Zugangspunkte, um über VPN auf Firmendaten zugreifen zu können. Die bereits eingerichtete Internet-Verbindung etwa vom Home-Office-Arbeitsplatz eines Außendienstmitarbeiters aus ist dabei nur eine Zugangsmöglichkeit, wird aber von vielen VPN Clients als Standardverbindung angenommen. NCP engineering empfiehlt daher eine Software, die sich nicht nur um VPN-Verschlüsselung und die Verbindung kümmert, sondern auch die richtige Verbindungsart auszuwählen vermag.

Foto: (c) PictureArt\_Fotolia



### **Zentrales Management**

Tipp 1: Die Einrichtung von Remote Access bringt ohne Frage einen gewissen Verwaltungsaufwand für den Systemadministratoren mit sich. Dabei müssen Aspekte wie die Einrichtung der VPN-Clients, die Art der Authentifizierung, Endpoint-Security-Check und die Art Zugangs etwa über Mobilfunk oder WLAN berücksichtigt werden. Das klingt kompliziert, ist es aber nicht, meinen die Experten von NCP engineering - sofern eine Lösung zum Einsatz kommt, mit der sich ein Remote Access-Netzwerk über eine zentrale Konsole administrieren lässt. Eine solche VPN Client Suite erlaubt die weitgehend automatische Einrichtung und Betreuung des Fernzugangsnetzwerks.

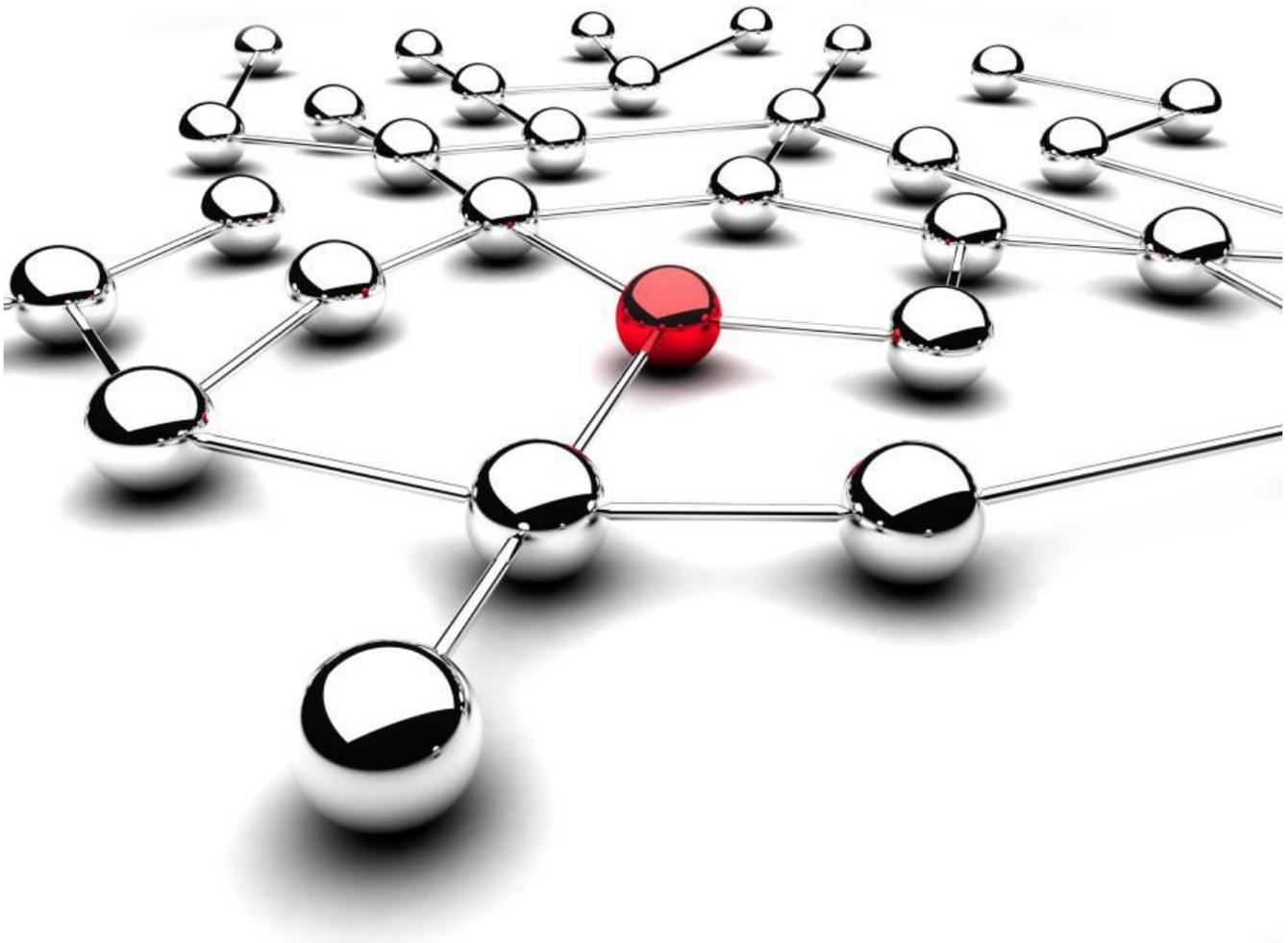
Foto: (c) Phoenixpix\_Fotolia



### **Vorsicht Kostenfalle**

Tipp 2: Zwar sind VPN-Softwarepakete in der Anschaffung relativ günstig, ihre Nutzung zieht jedoch Folgekosten nach sich, die viele Anwender oft übersehen, warnt NCP engineering. Der Betrieb einer Firewall etwa, die Erstellung einer Dokumentation, die Schulung von Nutzern, Updates und vieles mehr können die wahren Kosten einer Remote-Access-Lösung in die Höhe treiben. Um die Kosten in der Produktivphase im Griff zu behalten, empfehlen die Remote-Spezialisten von NCP engineering eine Lösung mit hohem Automatisierungsgrad. Je weniger Klicks End-User und Administratoren benötigen, um eine VPN-Verbindung aufzubauen, um so besser.

Foto: (c) Michael Nivelet\_Fotolia



### **Stabile Verbindung herstellen**

Tipp 3: Viele VPN-Systeme benötigen zahlreiche Klicks zur Herstellung einer Verbindung, die wertvolle Arbeitszeit kostet. Hier kann eine „One-Klick-Lösung“ helfen, bei der der User per Button-Klick eine Software aktiviert, die vom Aufbau der Verbindung bis zur Anpassung der Firewall-Regeln alles regelt.

Tipp 4: WLAN-Hot-Spot sicher nutzen Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

Foto: (c) Phoenixpix\_Fotolia



#### **WLAN-Hot-Spot sicher nutzen**

Tip 4: Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

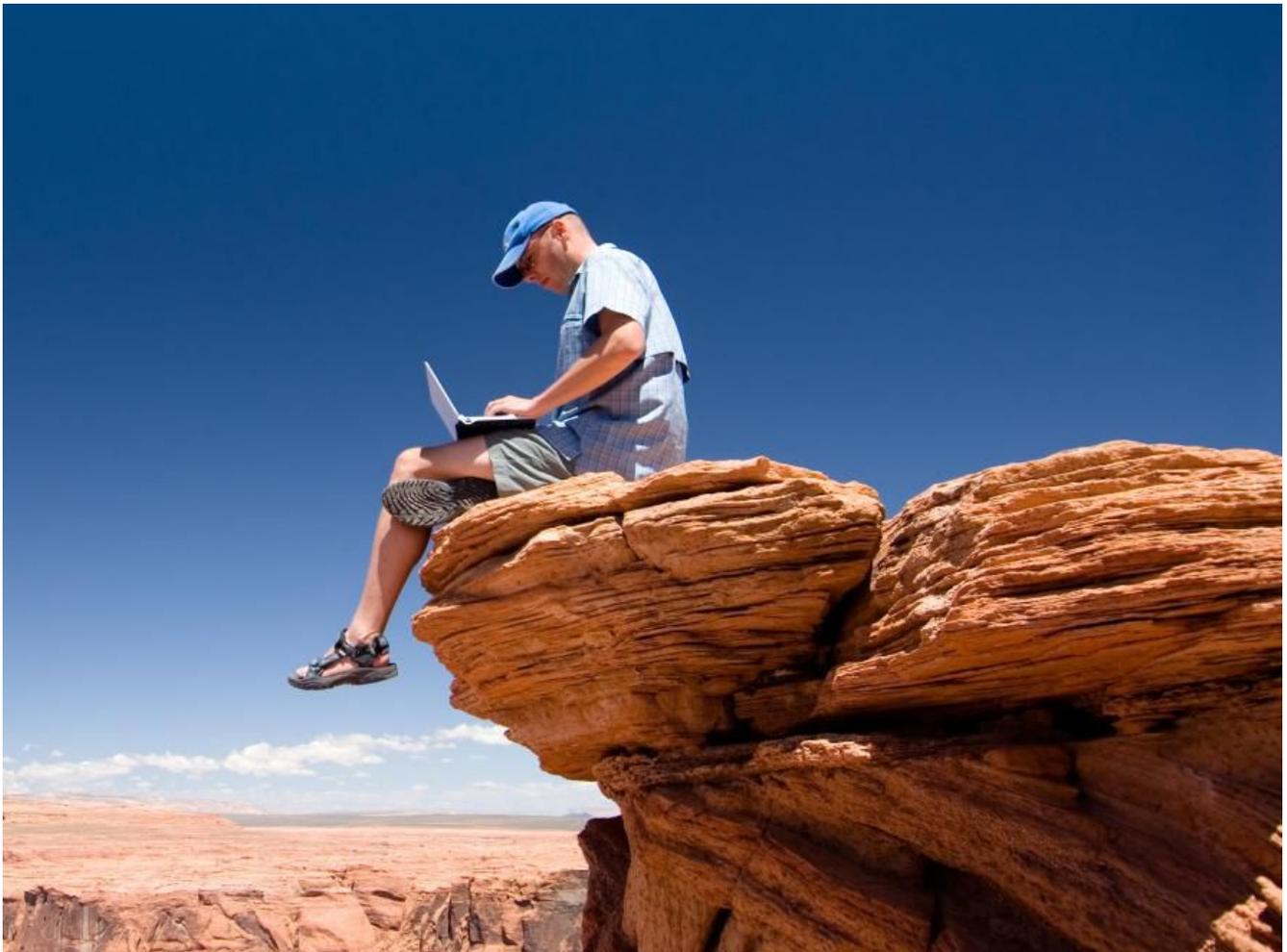
Foto: (c) WoGi\_Fotolia



#### **Kein Zugriff für User auf die Firewall:**

Tipp 5: Anders als von Anwendern vermutet, passen Personal Firewall-Einstellungen eines Client-Systems keineswegs für alle Remote-Access-Szenarien, mahnt NCP engineering. Ob nun öffentlicher WLAN-Hot-Spot oder Firmen-Außenstelle – unterschiedliche Remote-Access-Umgebungen erfordern unterschiedliche Firewall-Regeln. Und diese sollten von IT-Administrator vorgegeben werden, nicht vom User. Das senkt das Risiko von Bedienungsfehlern und das Sicherheitsrisiko.

Foto: (c) imageteam\_Fotolia



### **Automatische Verbindungswahl**

Tipp 6: Viele User nutzen je nach Aufenthaltsort verschiedene Zugangspunkte, um über VPN auf Firmendaten zugreifen zu können. Die bereits eingerichtete Internet-Verbindung etwa vom Home-Office-Arbeitsplatz eines Außendienstmitarbeiters aus ist dabei nur eine Zugangsmöglichkeit, wird aber von vielen VPN Clients als Standardverbindung angenommen. NCP engineering empfiehlt daher eine Software, die sich nicht nur um VPN-Verschlüsselung und die Verbindung kümmert, sondern auch die richtige Verbindungsart auszuwählen vermag.

Foto: (c) PictureArt\_Fotolia



### **Zentrales Management**

Tipp 1: Die Einrichtung von Remote Access bringt ohne Frage einen gewissen Verwaltungsaufwand für den Systemadministratoren mit sich. Dabei müssen Aspekte wie die Einrichtung der VPN-Clients, die Art der Authentifizierung, Endpoint-Security-Check und die Art Zugangs etwa über Mobilfunk oder WLAN berücksichtigt werden. Das klingt kompliziert, ist es aber nicht, meinen die Experten von NCP engineering - sofern eine Lösung zum Einsatz kommt, mit der sich ein Remote Access-Netzwerk über eine zentrale Konsole administrieren lässt. Eine solche VPN Client Suite erlaubt die weitgehend automatische Einrichtung und Betreuung des Fernzugangsnetzwerks.

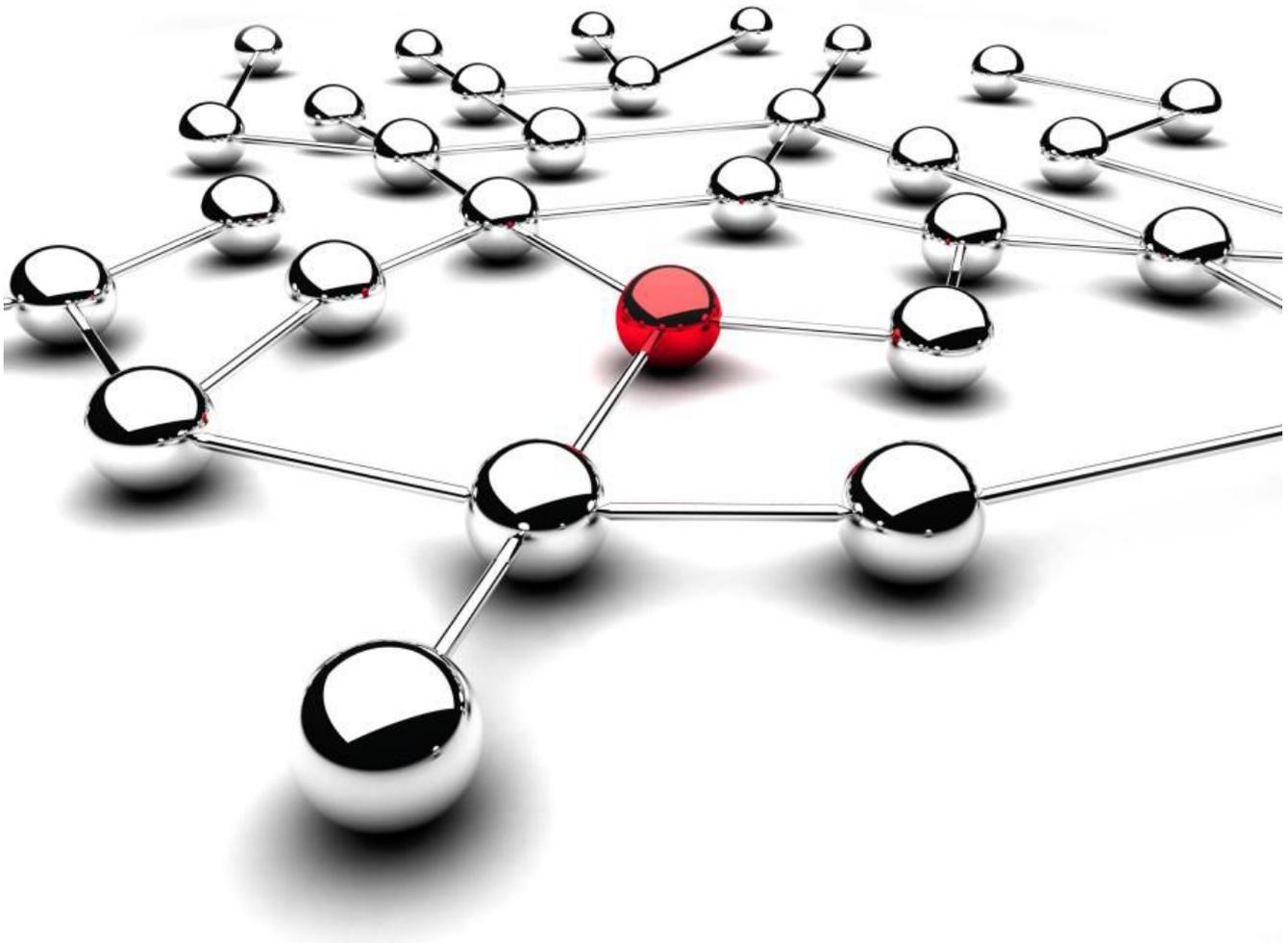
Foto: (c) Phoenixpix\_Fotolia



### **Vorsicht Kostenfalle**

Tipp 2: Zwar sind VPN-Softwarepakete in der Anschaffung relativ günstig, ihre Nutzung zieht jedoch Folgekosten nach sich, die viele Anwender oft übersehen, warnt NCP engineering. Der Betrieb einer Firewall etwa, die Erstellung einer Dokumentation, die Schulung von Nutzern, Updates und vieles mehr können die wahren Kosten einer Remote-Access-Lösung in die Höhe treiben. Um die Kosten in der Produktivphase im Griff zu behalten, empfehlen die Remote-Spezialisten von NCP engineering eine Lösung mit hohem Automatisierungsgrad. Je weniger Klicks End-User und Administratoren benötigen, um eine VPN-Verbindung aufzubauen, um so besser.

Foto: (c) Michael Nivelet\_Fotolia



### **Stabile Verbindung herstellen**

Tipp 3: Viele VPN-Systeme benötigen zahlreiche Klicks zur Herstellung einer Verbindung, die wertvolle Arbeitszeit kostet. Hier kann eine „One-Klick-Lösung“ helfen, bei der der User per Button-Klick eine Software aktiviert, die vom Aufbau der Verbindung bis zur Anpassung der Firewall-Regeln alles regelt.

Tipp 4: WLAN-Hot-Spot sicher nutzen Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

Foto: (c) Phoenixpix\_Fotolia



#### **WLAN-Hot-Spot sicher nutzen**

Tip 4: Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

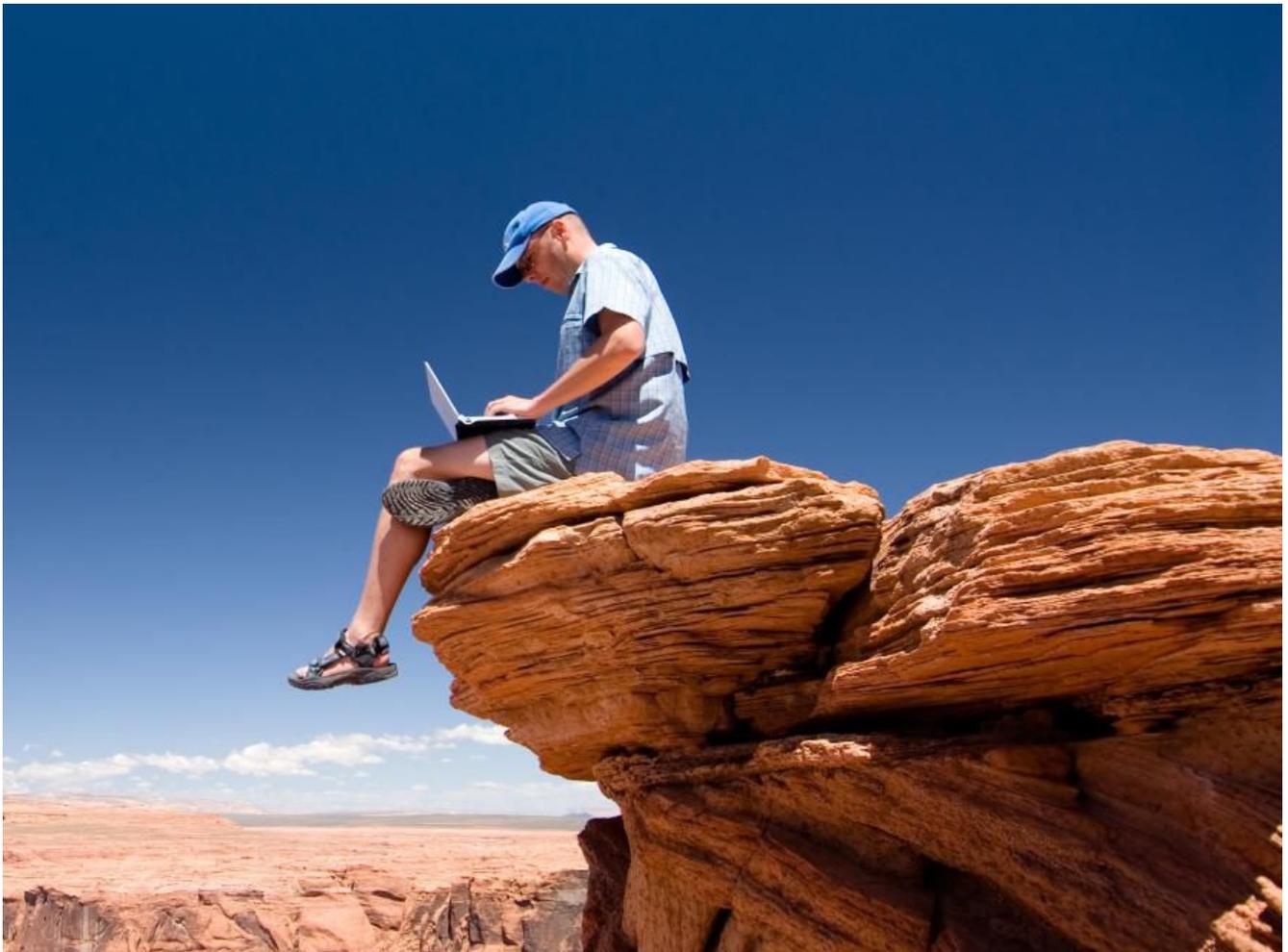
Foto: (c) WoGi\_Fotolia



#### **Kein Zugriff für User auf die Firewall:**

Tipp 5: Anders als von Anwendern vermutet, passen Personal Firewall-Einstellungen eines Client-Systems keineswegs für alle Remote-Access-Szenarien, mahnt NCP engineering. Ob nun öffentlicher WLAN-Hot-Spot oder Firmen-Außenstelle - unterschiedliche Remote-Access-Umgebungen erfordern unterschiedliche Firewall-Regeln. Und diese sollten von IT-Administrator vorgegeben werden, nicht vom User. Das senkt das Risiko von Bedienungsfehlern und das Sicherheitsrisiko.

Foto: (c) imageteam\_Fotolia



### **Automatische Verbindungswahl**

Tipp 6: Viele User nutzen je nach Aufenthaltsort verschiedene Zugangspunkte, um über VPN auf Firmendaten zugreifen zu können. Die bereits eingerichtete Internet-Verbindung etwa vom Home-Office-Arbeitsplatz eines Außendienstmitarbeiters aus ist dabei nur eine Zugangsmöglichkeit, wird aber von vielen VPN Clients als Standardverbindung angenommen. NCP engineering empfiehlt daher eine Software, die sich nicht nur um VPN-Verschlüsselung und die Verbindung kümmert, sondern auch die richtige Verbindungsart auszuwählen vermag.

Foto: (c) PictureArt\_Fotolia



### **Zentrales Management**

Tipp 1: Die Einrichtung von Remote Access bringt ohne Frage einen gewissen Verwaltungsaufwand für den Systemadministratoren mit sich. Dabei müssen Aspekte wie die Einrichtung der VPN-Clients, die Art der Authentifizierung, Endpoint-Security-Check und die Art Zugangs etwa über Mobilfunk oder WLAN berücksichtigt werden. Das klingt kompliziert, ist es aber nicht, meinen die Experten von NCP engineering - sofern eine Lösung zum Einsatz kommt, mit der sich ein Remote Access-Netzwerk über eine zentrale Konsole administrieren lässt. Eine solche VPN Client Suite erlaubt die weitgehend automatische Einrichtung und Betreuung des Fernzugangsnetzwerks.

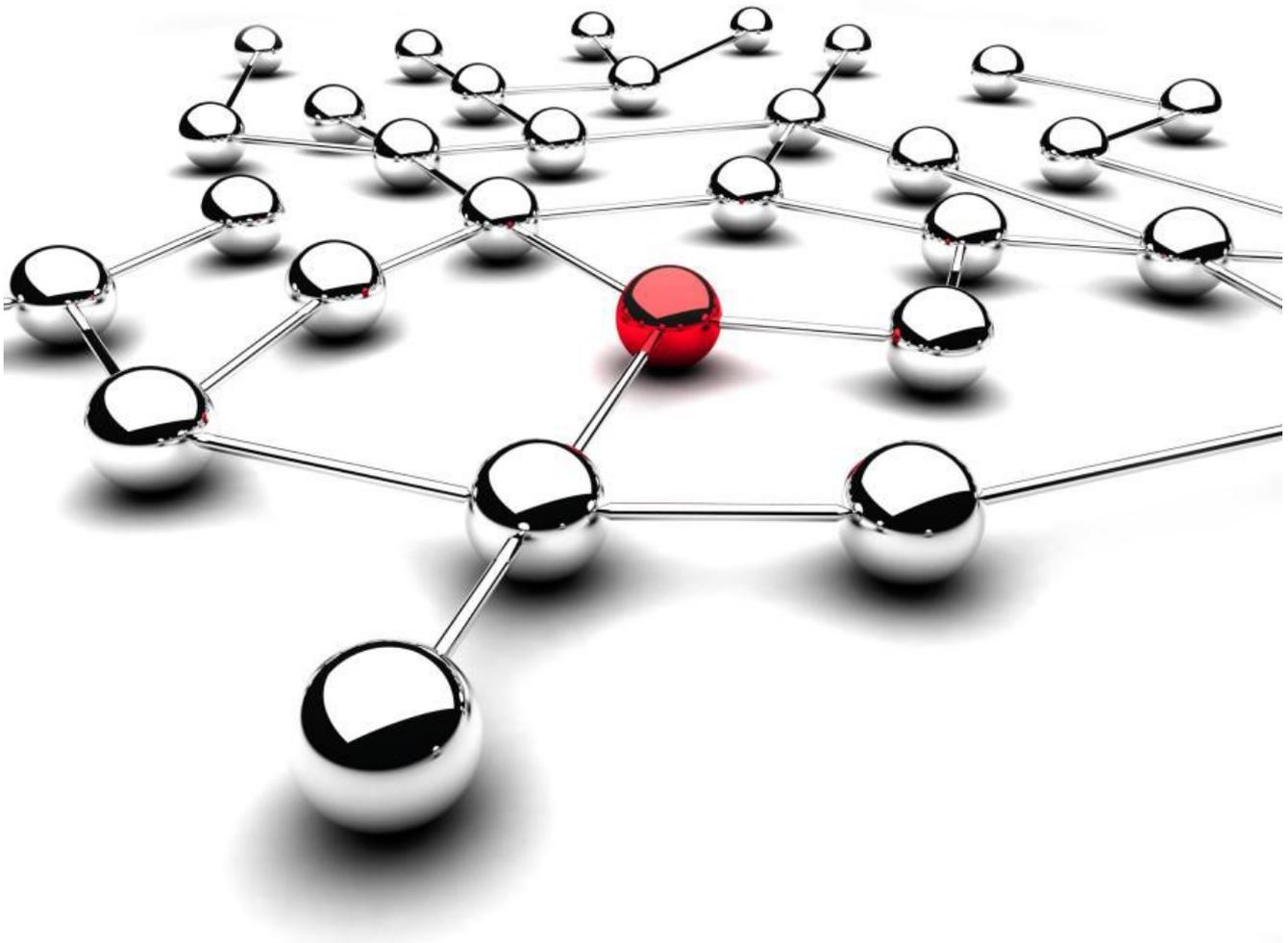
Foto: (c) Phoenixpix\_Fotolia



### **Vorsicht Kostenfalle**

Tipp 2: Zwar sind VPN-Softwarepakete in der Anschaffung relativ günstig, ihre Nutzung zieht jedoch Folgekosten nach sich, die viele Anwender oft übersehen, warnt NCP engineering. Der Betrieb einer Firewall etwa, die Erstellung einer Dokumentation, die Schulung von Nutzern, Updates und vieles mehr können die wahren Kosten einer Remote-Access-Lösung in die Höhe treiben. Um die Kosten in der Produktivphase im Griff zu behalten, empfehlen die Remote-Spezialisten von NCP engineering eine Lösung mit hohem Automatisierungsgrad. Je weniger Klicks End-User und Administratoren benötigen, um eine VPN-Verbindung aufzubauen, um so besser.

Foto: (c) Michael Nivelet\_Fotolia



### **Stabile Verbindung herstellen**

Tipp 3: Viele VPN-Systeme benötigen zahlreiche Klicks zur Herstellung einer Verbindung, die wertvolle Arbeitszeit kostet. Hier kann eine „One-Klick-Lösung“ helfen, bei der der User per Button-Klick eine Software aktiviert, die vom Aufbau der Verbindung bis zur Anpassung der Firewall-Regeln alles regelt.

Tipp 4: WLAN-Hot-Spot sicher nutzen Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

Foto: (c) Phoenixpix\_Fotolia



#### **WLAN-Hot-Spot sicher nutzen**

Tip 4: Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

Foto: (c) WoGi\_Fotolia



#### **Kein Zugriff für User auf die Firewall:**

Tipp 5: Anders als von Anwendern vermutet, passen Personal Firewall-Einstellungen eines Client-Systems keineswegs für alle Remote-Access-Szenarien, mahnt NCP engineering. Ob nun öffentlicher WLAN-Hot-Spot oder Firmen-Außenstelle – unterschiedliche Remote-Access-Umgebungen erfordern unterschiedliche Firewall-Regeln. Und diese sollten von IT-Administrator vorgegeben werden, nicht vom User. Das senkt das Risiko von Bedienungsfehlern und das Sicherheitsrisiko.

Foto: (c) imageteam\_Fotolia



### **Automatische Verbindungswahl**

Tipp 6: Viele User nutzen je nach Aufenthaltsort verschiedene Zugangspunkte, um über VPN auf Firmendaten zugreifen zu können. Die bereits eingerichtete Internet-Verbindung etwa vom Home-Office-Arbeitsplatz eines Außendienstmitarbeiters aus ist dabei nur eine Zugangsmöglichkeit, wird aber von vielen VPN Clients als Standardverbindung angenommen. NCP engineering empfiehlt daher eine Software, die sich nicht nur um VPN-Verschlüsselung und die Verbindung kümmert, sondern auch die richtige Verbindungsart auszuwählen vermag.

Foto: (c) PictureArt\_Fotolia



### **Zentrales Management**

Tipp 1: Die Einrichtung von Remote Access bringt ohne Frage einen gewissen Verwaltungsaufwand für den Systemadministratoren mit sich. Dabei müssen Aspekte wie die Einrichtung der VPN-Clients, die Art der Authentifizierung, Endpoint-Security-Check und die Art Zugangs etwa über Mobilfunk oder WLAN berücksichtigt werden. Das klingt kompliziert, ist es aber nicht, meinen die Experten von NCP engineering - sofern eine Lösung zum Einsatz kommt, mit der sich ein Remote Access-Netzwerk über eine zentrale Konsole administrieren lässt. Eine solche VPN Client Suite erlaubt die weitgehend automatische Einrichtung und Betreuung des Fernzugangsnetzwerks.

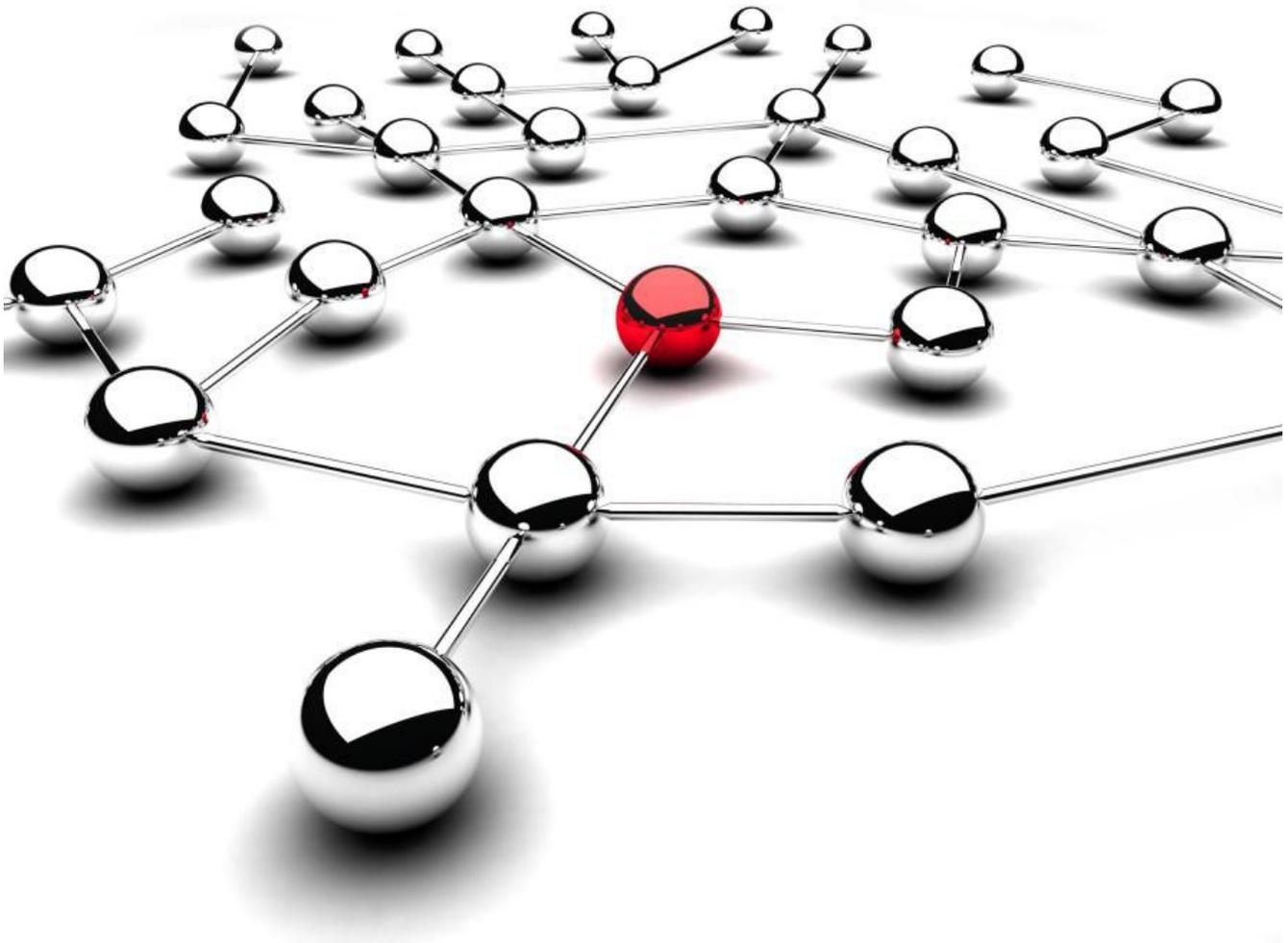
Foto: (c) Phoenixpix\_Fotolia



### **Vorsicht Kostenfalle**

Tipp 2: Zwar sind VPN-Softwarepakete in der Anschaffung relativ günstig, ihre Nutzung zieht jedoch Folgekosten nach sich, die viele Anwender oft übersehen, warnt NCP engineering. Der Betrieb einer Firewall etwa, die Erstellung einer Dokumentation, die Schulung von Nutzern, Updates und vieles mehr können die wahren Kosten einer Remote-Access-Lösung in die Höhe treiben. Um die Kosten in der Produktivphase im Griff zu behalten, empfehlen die Remote-Spezialisten von NCP engineering eine Lösung mit hohem Automatisierungsgrad. Je weniger Klicks End-User und Administratoren benötigen, um eine VPN-Verbindung aufzubauen, um so besser.

Foto: (c) Michael Nivelet\_Fotolia



### **Stabile Verbindung herstellen**

Tipp 3: Viele VPN-Systeme benötigen zahlreiche Klicks zur Herstellung einer Verbindung, die wertvolle Arbeitszeit kostet. Hier kann eine „One-Klick-Lösung“ helfen, bei der der User per Button-Klick eine Software aktiviert, die vom Aufbau der Verbindung bis zur Anpassung der Firewall-Regeln alles regelt.

Tipp 4: WLAN-Hot-Spot sicher nutzen Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

Foto: (c) Phoenixpix\_Fotolia



#### **WLAN-Hot-Spot sicher nutzen**

Tip 4: Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

Foto: (c) WoGi\_Fotolia



#### **Kein Zugriff für User auf die Firewall:**

Tipp 5: Anders als von Anwendern vermutet, passen Personal Firewall-Einstellungen eines Client-Systems keineswegs für alle Remote-Access-Szenarien, mahnt NCP engineering. Ob nun öffentlicher WLAN-Hot-Spot oder Firmen-Außenstelle - unterschiedliche Remote-Access-Umgebungen erfordern unterschiedliche Firewall-Regeln. Und diese sollten von IT-Administrator vorgegeben werden, nicht vom User. Das senkt das Risiko von Bedienungsfehlern und das Sicherheitsrisiko.

Foto: (c) imageteam\_Fotolia



### **Automatische Verbindungswahl**

Tipp 6: Viele User nutzen je nach Aufenthaltsort verschiedene Zugangspunkte, um über VPN auf Firmendaten zugreifen zu können. Die bereits eingerichtete Internet-Verbindung etwa vom Home-Office-Arbeitsplatz eines Außendienstmitarbeiters aus ist dabei nur eine Zugangsmöglichkeit, wird aber von vielen VPN Clients als Standardverbindung angenommen. NCP engineering empfiehlt daher eine Software, die sich nicht nur um VPN-Verschlüsselung und die Verbindung kümmert, sondern auch die richtige Verbindungsart auszuwählen vermag.

Foto: (c) PictureArt\_Fotolia



### **Zentrales Management**

Tipp 1: Die Einrichtung von Remote Access bringt ohne Frage einen gewissen Verwaltungsaufwand für den Systemadministratoren mit sich. Dabei müssen Aspekte wie die Einrichtung der VPN-Clients, die Art der Authentifizierung, Endpoint-Security-Check und die Art Zugangs etwa über Mobilfunk oder WLAN berücksichtigt werden. Das klingt kompliziert, ist es aber nicht, meinen die Experten von NCP engineering - sofern eine Lösung zum Einsatz kommt, mit der sich ein Remote Access-Netzwerk über eine zentrale Konsole administrieren lässt. Eine solche VPN Client Suite erlaubt die weitgehend automatische Einrichtung und Betreuung des Fernzugangsnetzwerks.

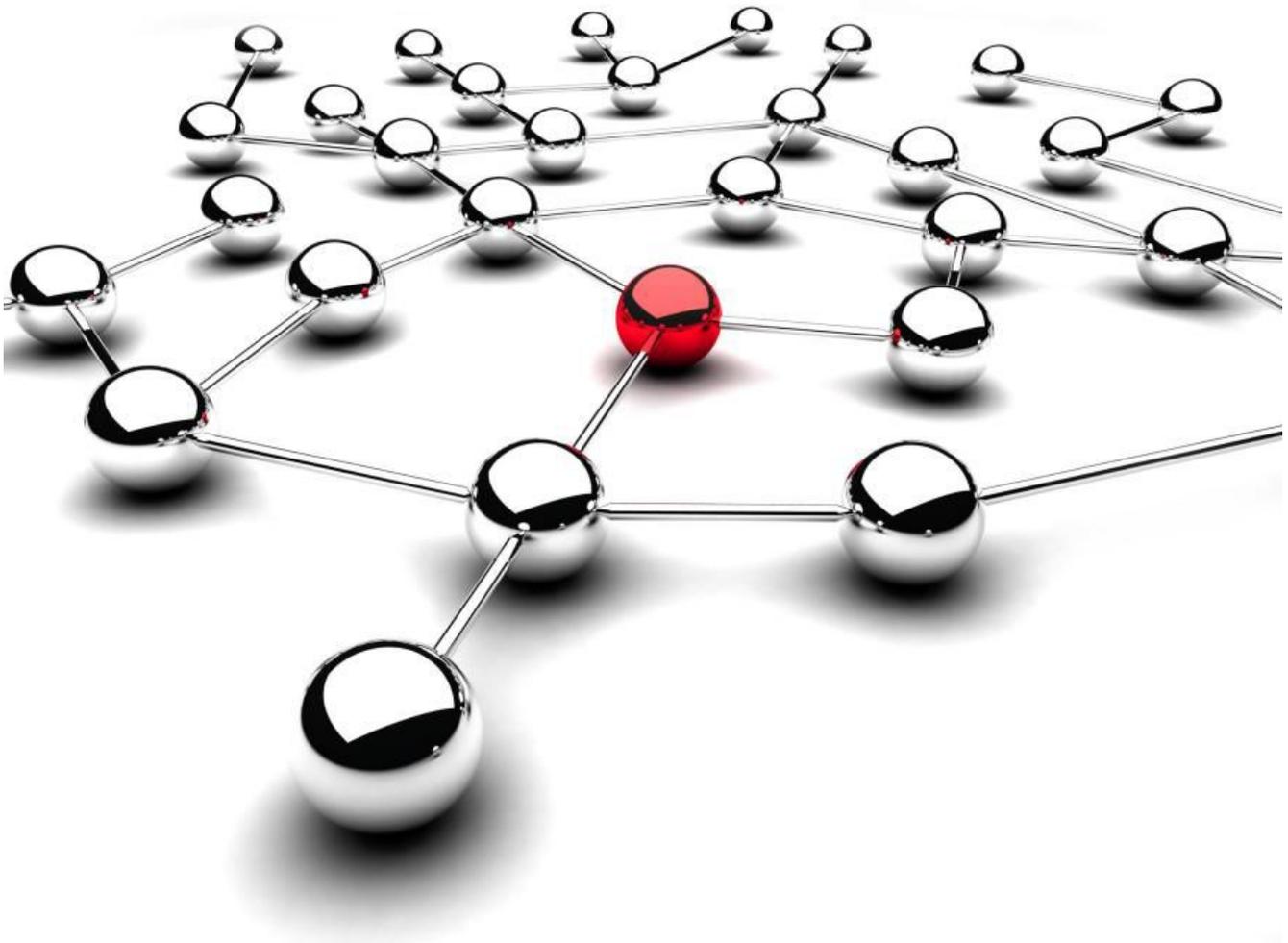
Foto: (c) Phoenixpix\_Fotolia



### **Vorsicht Kostenfalle**

Tipp 2: Zwar sind VPN-Softwarepakete in der Anschaffung relativ günstig, ihre Nutzung zieht jedoch Folgekosten nach sich, die viele Anwender oft übersehen, warnt NCP engineering. Der Betrieb einer Firewall etwa, die Erstellung einer Dokumentation, die Schulung von Nutzern, Updates und vieles mehr können die wahren Kosten einer Remote-Access-Lösung in die Höhe treiben. Um die Kosten in der Produktivphase im Griff zu behalten, empfehlen die Remote-Spezialisten von NCP engineering eine Lösung mit hohem Automatisierungsgrad. Je weniger Klicks End-User und Administratoren benötigen, um eine VPN-Verbindung aufzubauen, um so besser.

Foto: (c) Michael Nivelet\_Fotolia



### **Stabile Verbindung herstellen**

Tip 3: Viele VPN-Systeme benötigen zahlreiche Klicks zur Herstellung einer Verbindung, die wertvolle Arbeitszeit kostet. Hier kann eine „One-Klick-Lösung“ helfen, bei der der User per Button-Klick eine Software aktiviert, die vom Aufbau der Verbindung bis zur Anpassung der Firewall-Regeln alles regelt.

Tip 4: WLAN-Hot-Spot sicher nutzen Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Acces-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

Foto: (c) Phoenixpix\_Fotolia



#### **WLAN-Hot-Spot sicher nutzen**

Tip 4: Die Sorge der IT-Verantwortlichen vor Hackern, die über potenziell unsichere Netzwerke wie WLAN-Hot-Spots auf das Firmennetzwerk zugreifen, ist aus Sicht von NCP engineering unbegründet. Voraussetzung dafür ist eine Firewall, die sich automatisch an die jeweilige Remote-Access-Umgebung anpasst, deren Regeln dabei aber vom Administrator zentral vorgegeben werden, so dass der Anwender sie weder verändern noch außer Kraft setzen kann.

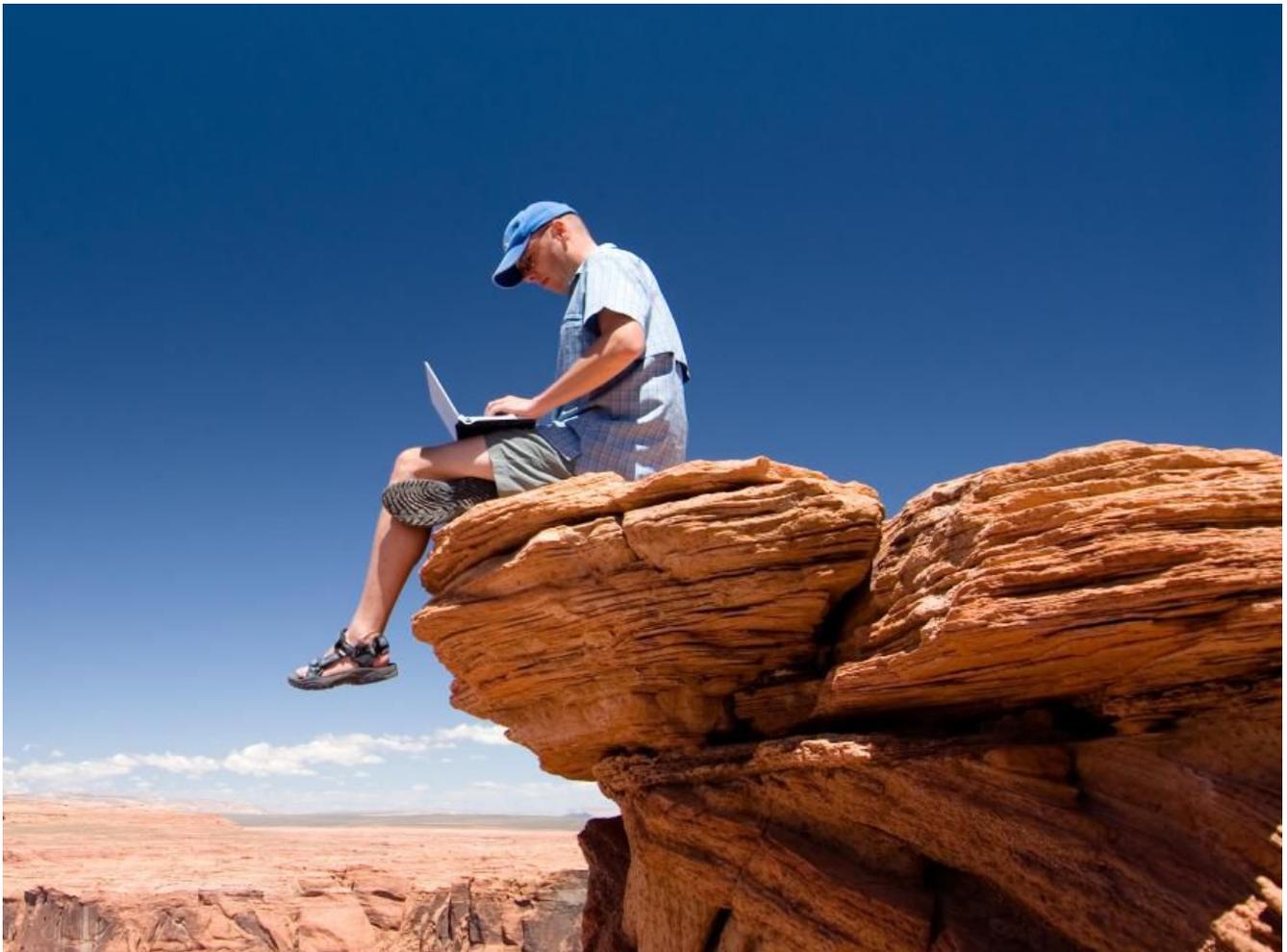
Foto: (c) WoGi\_Fotolia



#### **Kein Zugriff für User auf die Firewall:**

Tipp 5: Anders als von Anwendern vermutet, passen Personal Firewall-Einstellungen eines Client-Systems keineswegs für alle Remote-Access-Szenarien, mahnt NCP engineering. Ob nun öffentlicher WLAN-Hot-Spot oder Firmen-Außenstelle – unterschiedliche Remote-Access-Umgebungen erfordern unterschiedliche Firewall-Regeln. Und diese sollten von IT-Administrator vorgegeben werden, nicht vom User. Das senkt das Risiko von Bedienungsfehlern und das Sicherheitsrisiko.

Foto: (c) imageteam\_Fotolia



### **Automatische Verbindungswahl**

Tipp 6: Viele User nutzen je nach Aufenthaltsort verschiedene Zugangspunkte, um über VPN auf Firmendaten zugreifen zu können. Die bereits eingerichtete Internet-Verbindung etwa vom Home-Office-Arbeitsplatz eines Außendienstmitarbeiters aus ist dabei nur eine Zugangsmöglichkeit, wird aber von vielen VPN Clients als Standardverbindung angenommen. NCP engineering empfiehlt daher eine Software, die sich nicht nur um VPN-Verschlüsselung und die Verbindung kümmert, sondern auch die richtige Verbindungsart auszuwählen vermag.

Foto: (c) PictureArt\_Fotolia

---

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.