★ Dieser Artikel ist in **Zusammenarbeit mit NCP** entstanden.

Ist Ihr Unternehmen fit für die Homeoffice-Zukunft? **Machen Sie den 3-Punkte-Check!**

Homeoffice ist als flexibles Arbeitsmodell nicht mehr wegzudenken. Finden Sie mit drei einfachen Fragen heraus, ob Ihre Infrastruktur dafür gut ausgerichtet ist!

Text Dennis Christ, Content Marketing Manager, NCP engineering GmbH

NCP SECURE COMMUNICATIONS

NCP ist IT-Sicherheit „Made in Germany"! Vom Einzelanwender bis hin zu tausenden Nutzern im Großkonzern bieten wir die passende VPN-Software-Lösung. Unsere Produkte profitieren von über 30 Jahren im IT-Security-Umfeld und punkten mit schneller Inbetriebnahme, maximaler Skalierbarkeit und geprüfter Sicherheit nach der Norm ISO 9001. Profitieren Sie von unseren flexiblen Lizenzmodellen wie Pay-per-Use, Temporary Use oder Software-Subscription.

Homeoffice und Remote Work werden künftig ein wichtiger Teil der Arbeitswelt bleiben. Laut einer aktuellen Bitkom-Studie arbeiteten bereits im Dezember 2020 rund 10,5 Millionen Deutsche überwiegend von Zuhause. 75 Prozent aller Arbeitnehmer denken, dass Homeoffice in Deutschland zukünftig noch deutlich mehr genutzt werden sollte.

Der Bedarf an Remote-Work-Optionen kann und wird also künftig weiter zunehmen. Arbeitgeber müssen auch nach der Pandemie z.B. bei Schneechaos ihrer Belegschaft ermöglichen, aus dem Homeoffice heraus produktiv zu sein. Unternehmen sollten sich genau jetzt die Frage stellen, ob die eigene Remote-Access-Infrastruktur dafür bereit ist – machen Sie den Test mit drei einfachen Fragen!

1 Können Sie schnell reagieren?

„Homeoffice überall da, wo es möglich ist!", so lautete der jüngste Beschluss. Von einem Tag auf den anderen soll die komplette Belegschaft geschlossen ins Homeoffice umziehen – hierfür muss die entsprechende Remote-Access- oder VPN-Lösung schnell einsatzbereit und nahtlos in die vorhandene Firmen-Infrastruktur integrierbar sein. Am besten eignen sich dafür softwarebasierte Lösungen mit universeller Kompatibilität …

- … zu Laptops, Tablets und Smartphones sowie
- … zu den gängigsten Betriebssystemen und weiteren Netzwerk-Komponenten wie Firewall-Lösungen.

Auf diese Weise ist keine zusätzliche Hardware nötig und die VPN Clients können zentral verwaltet und automatisiert per Ferninstallation auf den Endgeräten der Nutzer eingerichtet werden.

Mehr Informationen unter:
ncp-e.com/de

2 Können Sie auch künftig flexibel reagieren?

Auch langfristig sollten Sie nach der Erstinstallation flexibel bleiben. Das aktuelle Schneechaos zeigt, dass es immer wieder Phasen mit erhöhtem Homeoffice-Bedarf gibt. Idealerweise können Sie diesen wechselnden Bedarf regulieren, ohne dauerhaft für die maximale Anzahl an Lizenzen zu zahlen. Anbieter wie NCP bieten hierfür flexible „Pay per Use"-Modelle an.

Als Unternehmen erhalten Sie einen Grundstock an Lizenzen, der Ihren typischen Homeoffice-Bedarf deckt. Wenn jedoch spontan mehr Mitarbeiter von zuhause arbeiten müssen, können Sie jederzeit auf weitere Lizenzen zugreifen, um den erhöhten Bedarf zeitweise abzudecken. Das Zahlungsmodell richtet sich nach Ihrer wirklichen Nutzung. Auf diese Weise binden Sie immer genau so viele Anwender an wie es die jeweilige Situation erfordert, ohne für die gesamte Belegschaft Lizenzen kaufen oder langfristig mieten zu müssen.

3 Ist die Sicherheit Ihres Firmennetzwerkes IMMER sichergestellt?

Schnelligkeit und Flexibilität sind bei der Implementierung einer Remote-Access-Lösung zweifellos schlagende Argumente. Dennoch müssen sich IT-Administratoren zu jedem Zeitpunkt darauf verlassen können, dass die VPN-Lösung in erster Linie absolut verlässlich agiert und kein Sicherheitsrisiko darstellt. Eine zusätzliche Anhebung des Sicherheitslevels bieten hier Lösungen, welche die eingesetzten Endgeräte auf ihre Sicherheit und z.B. auf Aktualität des Betriebssystems oder Virenscanners überprüfen.

Zu empfehlen ist der Einsatz privater Endgeräte zwar nicht, gerade in der ersten Phase der Pandemie war dies aber oft aufgrund von Hardware-Engpässen eine gängige Notlösung. Endpoint Security Checks bieten an dieser Stelle zwar keine finale Sicherheit, können die Risiken aber zumindest weiter minimieren. Aus diesem Grund sollten entsprechende Remote-Access-Lösungen das Endgerät selbst vor jedem Verbindungsversuch auf mögliche Schwachstellen überprüfen. Ist die Firewall aktuell? Sind die neuesten Betriebssystem-Versionen installiert? Stimmen alle Lizenzen und Zertifikate? Falls sich hier ein potenzielles Einfallstor auftut, wird dem Nutzer vom System die Verbindung und damit der Zugriff auf das Firmennetzwerk verweigert.

Vertrauen Sie deutschen Herstellern

Es gibt deutsche Anbieter für IT-Security Lösungen wie NCP engineering aus Nürnberg, die sich dem Kundennutzen verschrieben haben – durch Lösungen, die schnell und unkompliziert implementiert werden können, sich mit flexiblen Modellen jedem Bedarf anpassen und die Risiken durch ein Höchstmaß an Sicherheit minimieren. ■

„Gerade in diesen Zeiten ist der Remote-Arbeitsplatz für uns besonders wichtig, um die elementaren Dinge für die Bevölkerung in Baden-Baden zu steuern."
Matthias Götz, IT-Leiter Stadtverwaltung Baden-Baden