

# SCHUTZ VON DATEN IN VERTEILTEN ARBEITS-UMGEBUNGEN

»Überall arbeiten, überall geschützt.«

## Die Argumente für den Einsatz von conpal LAN Crypt zum Schutz von Daten in verteilten Arbeits-Umgebungen:

»New Work« ist eine wichtige Philosophie für Unternehmen auf der Suche nach jungen und besonders qualifizierten Arbeitskräften. Die Generation der Digital Natives sucht Flexibilität und fordert die Möglichkeit zur Arbeit von Zuhause oder unterwegs. Sie legt Wert auf die Work-Life-Balance und modernste Technik. Jeder Zweite setzt seine eigenen Geräte für den Job ein.<sup>1</sup>

Um diese Mitarbeiter für sich zu gewinnen, müssen Unternehmen ihnen das nötige Umfeld bieten: eine flexible, leistungsfähige IT, die unabhängig von Standort und verwendetem Endgerät alle Funktionen bietet, die zur Collaboration nötig sind.

Doch wie kann die Sicherheit der Daten unter diesen Rahmenbedingungen gewährleistet werden?

<sup>1</sup> »Millennials at work: Reshaping the workplace«, PWC: <https://www.pwc.de/de/prozessoptimierung/assets/millennials-at-work-2011.pdf>

## PROBLEMFELDER

### Home Office

Selbst wenn ein Arbeitnehmer im Home Office einen Firmen-Rechner benutzt, entstehen Risiken. Ein VPN in die Zentrale schützt die Daten, verschlechtert aber oft die Qualität der Verbindung. Für Video- oder Telefonkonferenzen wird der sichere Datentunnel deswegen oft deaktiviert. Dateien, die in diesem Zustand über das Netz verschickt werden, sind ungesichert.

### Mobile Work

Auf dem Weg in die Firma, zu Terminen oder auf Events: Mobile Work flexibilisiert die Arbeit und macht Mitarbeiter effizienter. Dabei bewegen sie sich frei zwischen verschiedenen Netzen sowie Infrastrukturen und nutzen verschiedene Endgeräte. Der Schutz der Daten muss dabei gewährleistet bleiben.

### Auf Reisen

Reisen sind für viele junge Arbeitnehmer wichtig. Sie stehen ihrer Arbeit oft nicht mehr im Weg – und sei es nur, um im Notfall einzuspringen. Mit einem eigenen Gerät oder einem Firmenrechner, in einem offenen WLAN im Café oder Hotel. Die Sicherheit der Verbindung ist dabei nicht gegeben. Die Sicherheit der Daten muss es aber sein.

### Heterogene Clients und BYOD

Für Technik-affine Mitarbeiter ist es wichtig, Endgeräte und Apps der neusten Generation zu benutzen. Oft legen sie großen Wert darauf, ihre privaten Geräte zu verwenden. Das stellt Unternehmen vor die Herausforderung, ein gleichbleibendes Sicherheitsniveau aufrecht zu erhalten.

## Die Lösung: Verschlüsselung über alle Clients hinweg

Mit conpal LAN Crypt lassen sich Dateien regelbasiert verschlüsseln – egal, ob Sie auf dem Server im eigenen Netzwerk liegen, auf der Festplatte eines Arbeitsplatz-Rechners oder in der Cloud. Auch im Transit vom Server zum Smartphone, in die Cloud oder ins Home-Office bleibt dieser Schutz bestehen – egal, welche Endgeräte Ihre Mitarbeiter verwenden.

### Sichere Daten auf allen Endgeräten: Windows – Mac – iPhone – Android

Egal wo ihre Mitarbeiter arbeiten wollen. Egal welches Gerät sie bevorzugen:  
Mit conpal LAN Crypt bleiben ihre Daten sicher verschlüsselt.

So profitieren Sie von der Flexibilität und Effizienz verteilter Arbeit, ohne den Schutz ihrer Daten zu kompromittieren.

## Wollen Sie sehen, wie conpal LAN Crypt funktioniert?

Erfahren Sie mehr unter [lancrypt.conpal.de](http://lancrypt.conpal.de). Gerne demonstrieren wir Ihnen auch persönlich, wie Sie den rollenbasierten Zugriff auf Dateien ermöglichen können.

Nehmen Sie mit uns unter [SalesSupport@conpal.de](mailto:SalesSupport@conpal.de) oder +49 (0) 6102 / 751 98-77 Kontakt auf!

**conpal**

conpal GmbH | Dornhofstraße 67-69  
63263 Neu-Isenburg | [www.conpal.de](http://www.conpal.de)

Ihr Partner