genua.

# Secure Home Office

## Strategien und Lösungen für eine sichere und effiziente mobile Organisation

Mobile Infrastrukturen sowohl effizient als auch sicher zu betreiben, ist eine große Herausforderung für die IT. Dabei gilt es, vielfältige personelle, prozessuale und technologische Fragen zu beantworten und eine optimale Balance zwischen IT Security, Kosten, Funktionsfähigkeit und Flexibilität zu gewährleisten.

Secur|Ty made in Germany

Secur|Ty made in EU

# Home Office: Die größten IT-Sicherheitsrisiken

### 1. Private Systeme und Netzwerke

Für die Arbeit im Home Office werden häufig private Systeme eingesetzt, die den IT-Security-Standards nicht genügen und nicht professionell administriert werden. Aber auch Lösungen, die ausschließlich zu beruflichen Zwecken im Home Office verwendet werden, befinden sich teilweise in nicht ausreichend abgesicherten Netzwerken.

### 2. Drittanbieterplattformen

Externen Systemen und Plattformen, die z. B. für Videokonferenzen genutzt werden, werden immer wieder Sicherheitslücken und unzureichende Datenintegrität nachgewiesen. Eine hohe Transparenz, die notwendig ist, um die Sicherheitsvorkehrungen der Anbieter zu beurteilen, ist dabei nicht immer gegeben.

### 3. Improvisierte Workflows

Viele Organisationen haben wenig Erfahrung mit mobilen Infrastrukturen und angemessenen Workflows. Das betrifft insbesondere die Trennung zwischen privaten und Unternehmensdaten bei Austausch, Bearbeitung und Speicherung. So können Angreifer Daten korrumpieren, infizieren, oder Informationen unbemerkt abschöpfen.

### 4. Unsichere Remote Desktop Software

Um die unkontrollierte Nutzung privater Systeme zu vermeiden und die getrennte Datenhaltung zu gewährleisten, setzen viele Unternehmen auf Remote-Desktop-Lösungen. Dabei zählen diese zu den häufigsten Einfallstoren für Angreifer, insbesondere durch schwache und selten gewechselte Passwörter.

### 5. VPN-Nutzung über private Endgeräte

Virtual Private Networks (VPN) sind ein bewährter Ansatz, um kritische Daten zu schützen. Wenn jedoch kein Firmengerät zur Verfügung steht und der VPN-Zugang von einem privaten Rechner erfolgt, öffnet sich ein Angriffskanal. Ist der private Rechner kompromittiert, erhält der Angreifer über das VPN Zugang in das Firmennetz.

» Ist der Absprung von einem Home-Office-System in das Unternehmensnetz geschafft, agiert der Angreifer wie ein interner Nutzer. Sabotageaktionen, Datenmanipulation und Datendiebstahl sind dann erheblich einfacher erfolgreich zu realisieren als bei Angriffen von außen.

**Carsten Arzig,**
IT-Sicherheitsexperte, genua GmbH

# Die wichtigsten Hebel für das Secure Home Office

Bei der Absicherung von Arbeitsplätzen im Home Office gegen Cyberangriffe müssen organisatorische Strukturen, Verhaltensregeln und technologische Lösungen nahtlos ineinandergreifen.

## 1. Transparenz & Governance

Eine umfassende Home Office Security Governance setzt auf klar festgelegte Prozesse für die regelmäßige Kontrolle der Kommunikation, Datenträger und Endgeräte und definiert Verschlüsselung, Viren-Scan-Systeme, Authentifikation und Firewalls. Und sie schafft Transparenz über Qualifikationen, Zertifizierungen und Referenzen der IT-Partner.

## 2. Strategie & Mindset

Um flexibles Arbeiten zum integralen Teil der Organisation zu machen, müssen Updates an Prozessen und Technologien von einem kulturellen Wandel begleitet werden, der die Mitarbeiter für Sicherheitsrisiken durch Hacker-Angriffe, Spionage und Social Engineering sensibilisiert.

## 3. Secure Remote Desktop

Eine kosteneffiziente Möglichkeit zur Trennung von Unternehmens- und Privatdaten bieten Remote-Desktop-Lösungen mit Multifaktor-Absicherung. So können Mitarbeiter auf dem Firmenrechner Daten bearbeiten und ausdrucken oder Mails lesen, ohne hohen Sicherheitsrisiken ausgesetzt zu sein.

## 4. Secure VPN

Ein mit dem Unternehmensnetz verbundenes VPN, auf das vom Home Office aus über einen geschützten Firmenrechner zugegriffen wird, bietet hohen Schutz und eine konsequente Datentrennung. Damit die Interaktion mit dem potenziell kompromittierten privaten Netzwerk ausgeschlossen werden kann, sollte entweder ein tief integriertes VPN realisiert werden, oder ein für hohe Sicherheitsanforderungen (etwa Geheimhaltungsgrad VS-NfD) zugelassenes Hardware-VPN.

## 5. Secure Boot

Eine weitere Lösung besteht im Booten eines vertrauenswürdigen und abgesicherten Betriebssystems von einem externen Medium, etwa einem Boot Stick. So kann das potenziell kompromittierte Betriebssystem des Privatrechners umgangen werden.

## Lösungen zur sicheren Anbindung mobiler Anwender

**VPN Software Client genuconnect Enterprise**
zur sicheren Anbindung von Laptops und Tablets mit MS Windows an Unternehmensnetze

**VPN Software Client genuconnect**
zur hochsicheren Anbindung von Laptops und Tablets mit MS Windows im Geheimschutzbereich

**Ecos Secure Boot Stick [SX]**
Plug & Play-Sicherheitslösung für flexible Telearbeit im Geheimschutzbereich

**iPhone-/iPad-Anbindung**
für mobiles Arbeiten via iOS Devices mit VS-NfD-Zulassung

**Weitere Informationen:**
www.genua.de/mobiles-arbeiten

# Secure Home Office: Top-Prioritäten für die IT-Sicherheit

1. **Multifaktor-Authentifizierung erweitern**
   Mitarbeiter im Home Office sollten eine Multifaktor-Authentifizierung für den Zugriff auf Netzwerke und kritische Anwendungen verwenden können.

2. **Netzwerk segmentieren**
   Das Netzwerk nach dem Prinzip „Zwiebelschalen“ in kritische und weniger kritische Bereiche unterteilen.

3. **Sicherheitsbewusstsein schärfen**
   Kritische Dienste vorkonfigurieren und Mitarbeiter mit klarer Kommunikation über Risiken informieren.

4. **VPNs strikt trennen**
   Einem via VPN mit dem Unternehmensnetzwerk verbundenen Gerät keinen gleichzeitigen Zugriff auf das ungeschützte lokale Netz bzw. das Internet gewähren.

5. **Teilnehmer in Online-Meetings identifizieren**
   Zu Beginn von Videokonferenzen sicherstellen, dass nur eingeladene Teilnehmer zugeschaltet sind.

6. **Patching für kritische Systeme sicherstellen**
   Möglichst kurze Patch-Zyklen für Systeme wie das VPN und den Endpunktschutz einrichten.

## Über genua

Die genua GmbH ist ein deutscher Spezialist für IT-Sicherheit. Seit der Firmengründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken und bieten hochwertige Lösungen. Unser Leistungsspektrum umfasst die Absicherung sensibler Schnittstellen im Behörden- und Industriebereich bis hin zur Vernetzung hochkritischer Infrastrukturen, die zuverlässig verschlüsselte Datenkommunikation via Internet, Fernwartungs-Systeme sowie Remote-Access-Lösungen für mobile Mitarbeiter und Home Offices. Unsere Lösungen werden in Deutschland entwickelt und produziert. Viele Firmen und Behörden setzen auf Lösungen von genua zum Schutz ihrer IT. genua ist ein Unternehmen der Bundesdruckerei-Gruppe.

**Weitere Informationen:**
www.genua.de/mobiles-arbeiten

**genua GmbH**
Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de

0324-01-DE