Smart Working & Cybersicherheit: KONVERTO macht's möglich

Neue Arbeitsweisen wie Homeoffice und Smart Working nehmen immer mehr in verschiedenen Unternehmen Einzug.
Um per Smart Working flexibel und effizient arbeiten zu können, reicht es nicht aus, die Mitarbeiter mit einer schnellen Internetanbindung, Laptop, Software und Headset auszustatten - neben geeigneten Collaboration-Tools sind Vorkehrungen zur nötigen Sicherheit zu treffen, maßgeblich.

Identifizierungssysteme & Cloud-Lösungen für mehr IT-Sicherheit
Die Eingrenzung der mit Smart Working verbundenen IT-Risiken für Unternehmen kann über konkrete Schutzmaßnahmen und technische Lösungen erfolgen:

- **Profilerstellung der Smart-Worker**
  Für ein Unternehmen ist es entscheidend, bereits im Voraus persönliche Benutzerprofile für alle Mitarbeiter im Homeoffice anzulegen. Abhängig vom festgelegten Aufgabengebiet gilt es daraufhin zu bestimmen, auf welche Informationen die Mitarbeiter zugreifen dürfen und welche Sicherheitsmechanismen definiert und angewandt werden sollen.

- **Authentifizierung der Fernzugriffe**
  Der erste Schritt zur Vermeidung fremder Eingriffe in das IT-System des Unternehmens besteht darin, ein Verfahren zur Identifizierung des Homeoffice-Arbeiters einzuführen, das greift, sobald sich dieser mit dem Unternehmenssystem verbindet. Idealerweise sollte man dabei auf die Mehrfachauthentifizierung setzen (Benutzername, Kennwort, einmalig nutzbarer Code usw.).

- **Trennung und Schutz der Hardware**
  Die einfachste Maßnahme zur Vermeidung der Gefahr einer Virenverseuchung zwischen der Hardware des Mitarbeiters und dem IT-System des Unternehmens besteht immer noch darin, dem Smart-Worker einen Computer zur ausschließlich beruflichen Nutzung zuzuweisen. Dieser muss vom IT-Personal regelmäßig auf das erforderliche Sicherheitsniveau aktualisiert werden. Auf dem von der Firma zur Verfügung gestellten Computer dürfen dem Anwender auch keine Administratorenrechte gewährt werden.

- **Sicherung des Datenzugriffs**
  Der Datenfluss zwischen dem Arbeitsplatz des Arbeitnehmers und dem Unternehmensnetz kann auch über VPN (Virtual Private Network) abgesichert werden. Auf vielen privaten Rechnern ist diese Sicherheitsvorrichtung jedoch nicht installiert.
  An sich kann man dieses Modell vorläufig durch die Nutzung einer mehrfach abgesicherten virtuellen Büroplattform via Cloud ersetzen. Diese Cloud-Plattformen ermöglichen es, von jedem beliebigen Ort und von jedem beliebigen Computer aus, auf sensible Unternehmensdaten zuzugreifen.

Was letzten Endes zählt, ist allerdings die Unversehrtheit der Firmendaten, die auf dem lokalen privaten Rechner gespeichert und verarbeitet werden, um anschließend ins Unternehmensnetz eingespeist zu werden. Deren Absicherung setzt eine ganze Reihe an Maßnahmen voraus, die Zeit für die Implementierung erfordern und die man bei privaten Geräten nur bedingt forcieren kann. Deshalb ist eine genaue Abstimmung mit dem Homeoffice- oder mobilen Arbeitnehmer empfehlenswert.

Mit dem KONVERTO Modern Workplace ist standortunabhängiges und flexibles Arbeiten von zuhause aus, auf Reisen, im Meeting-Raum oder im Büro möglich.

Smart Working - wir machen's möglich
+jederzeit und überall flexibel arbeiten
+effziente und produktive Zusammenarbeit
+einfacher und schneller Kommunikations-austausch
+Einsparung von Personal- und Fixkosten
+Lieferung von Hardware
+verschiedene Microsoft-365-Lizensierungsoptionen
+kontinuierliches Backup und Datenschutz
+sichere Multifactor-Autenthisierung
+Einzelcoachings und Teamtrainings

Nutzen Sie schon heute die Arbeitsform von morgen!
Melden Sie sich unter 800 031 031 und lassen Sie sich beraten.

KONVERTO AG | S.p.A. via Bruno-Buozzi-Str. 8, 39100 Bozen | Bolzano
Info Center 800 031 031 T 0471 064 500 info@konverto.eu info@pec.konverto.eu konverto.eu

Smart Working & Cyber Security: KONVERTO lo rende possibile

Nuovi metodi di lavoro come l'Home Office e lo Smart Working stanno diventando sempre più comuni in diverse aziende.
Per poter lavorare in modo flessibile ed efficiente attraverso lo Smart Working, non è sufficiente dotare i dipendenti di una connessione Internet veloce, di un portatile, un software e un headset - oltre a strumenti di collaborazione adeguati, è necessario prendere precauzioni per la necessaria sicurezza.

Sistemi di identificazione e soluzioni Cloud per una maggiore sicurezza IT
I rischi informatici per le aziende associate allo Smart Working possono essere contenuti mediante misure di protezione concrete e soluzioni tecniche:

- **Profili personali per gli Smart-Worker**
  Per un'azienda è fondamentale creare in anticipo i profili personali per tutti i dipendenti in Home Office. A seconda dell'area di attività definita, è quindi necessario determinare a quali informazioni i dipendenti possono accedere e quali meccanismi di sicurezza devono essere definiti e applicati.

- **Autenticazione degli accessi remoti**
  Il primo passo per impedire l'accesso non autorizzato al sistema informatico dell'azienda è l'implementazione di una procedura per l'identificazione del lavoratore in Home Office, che entra in vigore non appena il lavoratore si collega al sistema aziendale. Idealmente, questo dovrebbe basarsi su un'autenticazione multipla (nome utente, password, codice monouso, ecc.)

- **Separazione e protezione dell'hardware**
  Il modo più semplice per evitare il rischio di contaminazione da virus tra l'hardware del dipendente e il sistema informatico dell'azienda è quello di assegnare un computer per un uso esclusivamente professionale al dipendente. Questo computer deve essere regolarmente aggiornato dal personale informatico per garantire il livello di sicurezza richiesto. Sul computer messo a disposizione dall' azienda, all'utente non devono essere concessi diritti di amministratore.

- **Sicurezza dell'accesso ai dati**
  Il flusso di dati tra il posto di lavoro del dipendente e la rete aziendale può essere protetto anche tramite VPN (Virtual Private Network). Tuttavia, su molti computer privati questo dispositivo di sicurezza non è installato.
  Di per sé, questo modello può essere sostituito per il momento con l'utilizzo di una piattaforma di ufficio virtuale multi-secured via cloud. Queste piattaforme cloud consentono di accedere ai dati aziendali sensibili da qualsiasi luogo e da qualsiasi computer.

Ciò che conta infine, tuttavia, è l'integrità dei dati aziendali, che vengono memorizzati ed elaborati sul computer privato locale e poi immessi nella rete aziendale. La protezione di questi dati richiede tutta una serie di misure che richiedono tempo per essere attuate e che possono essere applicate solo in misura limitata per gli apparecchi privati. Si raccomanda pertanto un preciso coordinamento con il dipendente in Home Office.

Con KONVERTO Modern Workplace, è possibile lavorare da casa, in viaggio, in sala riunioni o in ufficio, in modo flessibile e indipendente dalla posizione.

Smart Working - noi lo rendiamo possibile
+lavorare in modo flessibile in qualsiasi momento e ovunque
+cooperazione efficiente e produttiva
+comunicazione semplice e veloce
+risparmio di personale e costi fissi
+fornitura del hardware
+varie opzioni di licenza Microsoft 365
+ backup continuo e protezione dei dati
+autenticazione sicura a più fattori
+Coaching individuali formazione del team

Approfittate oggi del metodo di lavoro di domani!
Chiamate il numero 800 031 031 e fatevi consigliare da noi.

KONVERTO AG | S.p.A. via Bruno-Buozzi-Str. 8, 39100 Bozen | Bolzano
Info Center 800 031 031 T 0471 064 500 info@konverto.eu info@pec.konverto.eu konverto.eu