



Cyber Security

Im Homeoffice



Maßnahmen priorisieren:
Ihre Checkliste zur
Dringlichkeitsbewertung



Cybersecurity-Risiken im
Remote-Arbeitsplatz für
die Industrie



Wie Industrieunternehmen
sensible Daten und
Produktionszugänge
schützen





com-Datentechnik GmbH
Digitaler Technologiepartner



Inhaltsverzeichnis

Dieses Whitepaper beleuchtet die spezifischen Herausforderungen der **IT-Sicherheit im Home Office** für Unternehmen Ihrer Branche. Wir zeigen Ihnen, warum der Schutz Ihrer Daten und Zugänge im Remote-Arbeitsplatz keine nachrangige Aufgabe, sondern eine **strategische Notwendigkeit** ist. Unser Ziel ist es, Ihnen einen klaren Überblick über die Risiken zu geben und praxisnahe Maßnahmen an die Hand zu geben, um Ihre Home Office-Umgebung **resilient und sicher zu gestalten**. So können Sie die Chancen der Digitalisierung voll ausschöpfen, ohne die Kontrolle über Ihre kritischen Assets zu verlieren



Wir über uns

S.3-4



Cybersecurity-Risiken
im Remote-Arbeitsplatz
für die Industrie

S.5-6



Maßnahmen priorisieren:
Ihre Checkliste zur
Dringlichkeitsbewertung

S.7-8



kontakt@com-datentechnik.de



+49 (0)7641/9272-0



www.com-datentechnik.de



com-Datentechnik GmbH
Digitaler Technologiepartner

Wir als com-Datentechnik



Über uns

Wir sind seit über 15 Jahre in der IT Branche tätig und betreuen seither mittelständische Unternehmen.

Was wir machen

Wir sind spezialisiert auf Cybersecurity, Netzwerktechnik, deren Planung und Wartung.

Warum wir

Die Cyberbedrohungen ändern sich ständig. Deshalb investieren wir fortlaufend in die Weiterbildung unseres Teams. So bleiben wir stets über aktuelle Angriffsmethoden und innovative Schutztechnologien informiert.

Kontaktieren Sie uns

 +49 (0)7641/9272-0

 kontakt@com-datentechnik.de

 www.com-datentechnik.de



com-Datentechnik GmbH
Digitaler Technologiepartner

Autor: Dano Schoner



Über mich

Als zertifizierter BSI IT-Grundschatz-Praktiker bringe ich fundierte Kenntnisse in der Implementierung und Aufrechterhaltung von IT-Sicherheitsstandards mit.

Kontakt

Bei Fragen können Sie mir auch gerne ein E-Mail schreiben oder mich anrufen.



d.schoner@com-datentechnik.de



+49 (0)7641/9272-25

IT- Grundschatzpraktiker



Mein Motto

Ich bin stets bestrebt, mein Wissen im Bereich IT-Sicherheit zu erweitern und mich über aktuelle Bedrohungen und Schutzmaßnahmen auf dem Laufenden zu halten.



kontakt@com-datentechnik.de



+49 (0)7641/9272-0



www.com-datentechnik.de



Cybersecurity-Risiken im Remote-Arbeitsplatz für die Industrie

Die unsichtbaren Risiken der modernen Arbeitswelt für die Industrie!

Die Art und Weise, wie wir arbeiten, hat sich dramatisch verändert. Das Home Office, einst eine **flexible Option**, ist für viele Unternehmen und Mitarbeiter im Zuge globaler Entwicklungen zu einem festen Bestandteil des Arbeitsalltags geworden. Auch in **traditionell standortgebundenen Sektoren** wie der Spritzguss-, Fertigungs- oder Pharmaindustrie ist die Remote-Arbeit heute Realität – sei es für die Entwicklungsabteilung, das Management oder spezialisierte IT-Kräfte, die auf kritische Systeme zugreifen müssen.

Diese Flexibilität bringt unbestreitbare Vorteile mit sich, doch sie birgt auch eine neue Dimension von **Sicherheitsrisiken**, die oft unterschätzt werden. Während in den gesicherten Produktionsstätten und Bürogebäuden bereits **robuste IT-Sicherheitsstrategien** etabliert sind, erweitert das Home Office die Angriffsfläche Ihres Unternehmens exponentiell. Private Netzwerke, unsichere Heimrouter, gemeinsam genutzte Computer.





com-Datentechnik GmbH
Digitaler Technologiepartner

Gerade für
Industrieunternehmen sind die
Konsequenzen eines
Datenlecks oder eines
erfolgreichen Cyberangriffs
verheerend:



Verlust von
Produktionsgeheimnissen:
Ob es sich um patentierte
Spritzgussformen, geheime
Fertigungsabläufe oder
sensible pharmazeutische
Rezepturen handelt –
geistiges Eigentum ist Ihr
höchstes Gut. Ein Abfluss
dieser Daten kann
existenzbedrohend sein.



Betriebsunterbrechungen:
Wenn Angreifer über
Home Office-Zugänge in
Ihre Netzwerke
eindringen und
Produktionssysteme
kompromittieren, drohen
teure Ausfälle und
Lieferkettenprobleme, die
den gesamten Betrieb
zum Erliegen bringen
können.



Compliance-
Verletzungen: Streng
regulierte Branchen wie
die Pharmaindustrie
unterliegen hohen
Compliance-
Anforderungen (z.B.
GMP, GxP, FDA). Eine
unzureichende
Datensicherheit im
Home Office kann hier
zu massiven Strafen und
Reputationsschäden
führen.



Reputationsverlust und Vertrauensschaden:
Ein öffentlich bekannt gewordener
Sicherheitsvorfall untergräbt das Vertrauen von
Kunden, Partnern und Investoren.



kontakt@com-datentechnik.de



+49 (0)7641/9272-0



www.com-datentechnik.de

IT-Sicherheits-Checkliste Home Office und Mobiles Arbeiten



Verwendung von VPN

VPN-Verbindungen sind eine sehr gute Maßnahme zur Verbesserung der IT-Sicherheit. Diese müssen mindestens dann verwendet werden, wenn Beschäftigte von außerhalb der Firma auf das Netzwerk zugreifen.



Patch-Management

Häufig werden Geräte, die sich außerhalb des Firmenstandortes befinden einfach vergessen. Es ist wichtig, auch hier regelmäßig Updates einzuspielen um etwaige Sicherheitslücken zu schließen.



Mehrfaktorauthentifizierung VPN & Cloud Dienste

VPN Zugang zur Firma, oder auch zu Cloud Dienste wie z.B Microsoft 365 oder Google work space sollte eine Mehrfaktorauthentifizierung eingerichtet werden,



Einbindung des Backupkonzeptes

Auch im Backup-Konzept fehlt oft eine genaue Regelung für Geräte, die sich außerhalb des Firmenstandortes befinden. Um Datenverlust zu vermeiden, sind entsprechende Regelungen erforderlich.



IT-Sicherheitsrichtlinie für Homeoffice

Für die Arbeit von zu Hause aus oder für mobiles Arbeiten sollte im Unternehmen eine Richtlinie für IT-Sicherheitsmaßnahmen erstellt werden. Eine Kopie dieser Richtlinie muss jedem Mitarbeitenden, der von außerhalb des Firmenstandortes arbeitet, ausgehändigt werden. Der Erhalt sollte schriftlich bestätigt werden.



Trennung Privat / Geschäftlich

Für Mitarbeitende im Homeoffice oder im Außendienst muss technisch und / oder organisatorisch sichergestellt werden, dass die private und die geschäftliche Nutzung getrennt sind. Es sollte klare Richtlinien geben, ob und inwiefern beispielsweise das Internet privat genutzt werden darf.



Muss man machen



Sollte man machen



Kann man machen



com-Datentechnik GmbH
Digitaler Technologiepartner



www.com-datentechnik.de

+49 (0)7641/9272-0

kontakt@com-datentechnik.de

IT-Sicherheits-Checkliste Home Office und Mobiles Arbeiten

Definierte Datenhaltung

VPN-Verbindungen sind eine sehr gute Maßnahme zur Verbesserung der IT-Sicherheit. Diese müssen mindestens dann verwendet werden, wenn Beschäftigte von außerhalb der Firma auf das Netzwerk zugreifen.

Datenträgerverschlüsselung

Häufig werden Geräte, die sich außerhalb des Firmenstandortes befinden einfach vergessen. Es ist wichtig, auch hier regelmäßig Updates einzuspielen um etwaige Sicherheitslücken zu schließen.

Regelung für die Ausgabe/ Rücknahme von Hardware

Hierbei muss es sich nicht um eine komplexe Richtlinie handeln. Es könnte einfach schriftlich festgehalten werden, wer Hardware ausgeben darf und wie die Ausgabe zu dokumentieren ist (z. B. Ausgabeliste). Für die Rückgabe reicht vielleicht schon eine kurze Prüfung der Hardware durch die verantwortliche Person und eine Unterschrift.

Incident Response Plan für Home Office-Vorfälle

Klare Prozesse für die Reaktion auf Sicherheitsvorfälle, die im Remote-Umfeld auftreten.

Sicherstellung, dass Home Office-Setups den branchenspezifischen Vorschriften (z.B. GMP, ISO 27001) entsprechen.

Sicheres WLAN im Homeoffice

Wlan Passwort sollte mindestens 12 Zeichen lang sein Groß-kleinbuchstaben, zahlen und Sonderzeichen enthalten. Die verschlüsselung sollte WPA2 sein und WPS sollte deaktiviert werden, da es anfällig für Angriffe sein kann.

Mehrfactorauthentifizierung Endgeräte

Für alle Geräte, die sich außerhalb des Firmenstandortes befinden, sollte eine Mehrfaktorauthentifizierung eingerichtet werden.



Muss man machen



Sollte man machen



Kann man machen



com-Datentechnik GmbH
Digitaler Technologiepartner



www.com-datentechnik.de



+49 (0)7641/9272-0



kontakt@com-datentechnik.de



Unser Service

IT-Service

Wir überwachen und warten Ihre IT-Systeme, um Ihre **Infrastruktur** flexibel **zuzuschneiden** und problemlos mit Ihrem **Wachstum** zu skalieren.

IT-Systeme

Wir unterstützen Sie dabei, die perfekte **Hard- und Software** zu finden, die exakt auf Ihre **individuellen** Anforderungen **zugeschnitten** ist.

IT-Infrastruktur

Mit unserer Betreuung und **strategischen Optimierung** machen wir Ihre Infrastruktur fit für die Zukunft, sodass sie den **wachsenden Anforderungen** jederzeit gerecht wird.

Cloud-Service

Profitieren Sie von gehosteten Lösungen für **mehr Effizienz, Mobilität und Sicherheit**.

So arbeiten Sie smart, **flexibel** und mit dem guten Gefühl, dass Ihre **Daten geschützt** sind.

Planung IT-Infrastruktur

Mit unserer **Expertise** planen wir Ihre IT-Infrastrukturprojekte **jeder Komplexität**, um einen schnellen und störungsfreien Aufbau Ihrer Systeme zu ermöglichen.

Cybersecurity

Mit umfassenden **IT-Sicherheitslösungen** schützen wir Ihr Unternehmen und Ihre sensiblen Daten zuverlässig vor **Cyber-Bedrohungen**.

