

1 IT-Arbeitsplatz-Sicherheit von <https://www.profidata-it.de/>

1.1 Sicherheitsrisiken im Homeoffice – Sind Sie wirklich geschützt?

The screenshot shows a webpage with the profidata IT logo and navigation menu. The main heading is "Sicherheitsrisiken im Homeoffice – Sind Sie wirklich geschützt?". Below this are four columns, each with an icon, a title, and a description of a security risk.


Icon	Risk Title	Description
	Unverschlüsselte Verbindungen	Jeden Tag, an dem Sie Ihre Verbindungen nicht schützen, riskieren Sie, dass vertrauliche Informationen in die falschen Hände geraten. Dies kann zu ernsthaften Datenschutzverletzungen (DSGVO) und potenziell hohen Bußgeldern führen.
	Schwache / Identische Passwörter	Benutzen Sie immer noch einfache Passwörter? Oder für jeden Zugang immer ein identisches Kennwort? Dann haben Hacker bei Ihnen ein sehr leichtes Spiel. Ein einziges schwaches Passwort kann Ihr gesamtes Netzwerk kompromittieren.
	Phishing-Angriffe Account Breach	Eine einzige unbedachte E-Mail und Ihre gesamten Unternehmensdaten könnten gestohlen werden. Aktuelle Phishing-Angriffe werden immer raffinierter und professioneller mit fast perfektem Inhalt. Sie zielen darauf ab, das Vertrauen und Unwissenheit der Mitarbeiter auszunutzen.
	Malware und Ransomware	Eine Infektion mit Malware oder Ransomware kann Ihre Systeme unmittelbar lahmlegen oder zerstören. Üblicherweise werden Ihre Daten oder Laufwerke verschlüsselt, sodass sie erst gegen Zahlung eines hohen Lösegelds wieder freigegeben werden.

1.2 Ihr Home-Arbeitsplatz könnte eine tickende Zeitbombe sein!

The screenshot shows a webpage with the profidata IT logo and navigation menu. The main heading is "Ihr Home-Arbeitsplatz könnte eine Zeitbombe sein!". Below the heading is a sub-heading: "Eine sichere IT-Umgebung ist das Fundament – Vernachlässigen Sie sie, und der Zusammenbruch droht!". The page features three images: a person holding a tablet displaying a security interface, a person working on a laptop with a security shield icon on the screen, and a smartphone displaying a VPN connection screen.

2 Denken Sie JETZT einfach mal über die folgenden Hinweise nach...

2.1 Überfliegen und prüfen Sie an Ihrem Arbeitsplatz



[profidata-IT](#) |
 [Kontakt](#) |
 [Sensor-Daten](#) |
 [Recht und Orga](#) |
 [Internes](#)

Denken Sie JETZT einfach mal über die folgenden Hinweise nach...

<p style="text-align: center;">Regelmäßige Updates</p> <p><i>Halten Sie Ihr Betriebssystem, Ihre Software und alle Anwendungen auf dem neuesten Stand, um Sicherheitslücken zu schließen.</i></p>	<p style="text-align: center;">Sichere Internet- und WLAN-Verbindung</p> <p><i>Verwenden Sie möglichst die WPA3-Verschlüsselung und ein starkes, einzigartiges Passwort für Ihr WLAN-Netzwerk.</i></p>	<p style="text-align: center;">Antiviren- und Antimalware-Software</p> <p><i>Installieren und aktualisieren Sie regelmäßig Antiviren- und Antimalware-Programme, um Ihr System vor Bedrohungen zu schützen.</i></p>
<p style="text-align: center;">Starke Passwörter</p> <p><i>Verwenden Sie komplexe, einzigartige Passwörter für alle Konten und implementieren Sie eine Passwort-Manager-Lösung.</i></p>	<p style="text-align: center;">Zwei-Faktor-Authentifizierung</p> <p><i>Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) für alle kritischen Konten und Zugänge, um eine zusätzliche Sicherheitsebene zu schaffen.</i></p>	<p style="text-align: center;">VPN-Nutzung</p> <p><i>Nutzen Sie ein Virtual Private Network (VPN) für sichere Verbindungen zum Firmennetzwerk und schützen Sie Ihre Datenübertragungen.</i></p>
<p style="text-align: center;">Sichere Datenspeicherung</p> <p><i>Verwenden Sie sichere Cloud-Dienste oder verschlüsselte externe Laufwerke für die Speicherung von Unternehmensdaten.</i></p>	<p style="text-align: center;">Netzwerk-Segmentierung</p> <p><i>Trennen Sie Arbeitsgeräte vom restlichen Heimnetzwerk, um die Sicherheit zu erhöhen.</i></p>	<p style="text-align: center;">Firewall-Aktivierung</p> <p><i>Stellen Sie sicher, dass sowohl Hardware- als auch Software-Firewalls aktiviert sind, um unerlaubten Zugriff zu verhindern.</i></p>
<p style="text-align: center;">USB-Sicherheit</p> <p><i>Beschränken Sie den Einsatz von USB-Geräten und nutzen Sie Sicherheitsmaßnahmen, um das Einschleppen von Malware zu verhindern.</i></p>	<p style="text-align: center;">IoT-Geräte-Sicherheit</p> <p><i>Stellen Sie sicher, dass alle internetfähigen Geräte (z.B. Smart-Home-Geräte) sicher konfiguriert und aktualisiert sind, um keine Einfallstore zu bieten.</i></p>	<p style="text-align: center;">Software-Berechtigungen</p> <p><i>Beschränken Sie die Installation und Ausführung von Software auf notwendige Anwendungen, um das Risiko von Sicherheitslücken zu minimieren.</i></p>
<p style="text-align: center;">Daten-Verschlüsselung</p> <p><i>Verschlüsseln Sie sensible Daten sowohl auf der Festplatte als auch während der Übertragung, um unbefugten Zugriff zu verhindern.</i></p>	<p style="text-align: center;">Regelmäßige Backups</p> <p><i>Implementieren Sie automatisierte Backup-Lösungen, um regelmäßig Sicherungskopien Ihrer wichtigen Daten zu erstellen und Datenverluste zu vermeiden.</i></p>	<p style="text-align: center;">Phishing-Schutz</p> <p><i>Schulen Sie sich und Ihre Mitarbeiter, um Phishing-E-Mails zu erkennen, und verwenden Sie E-Mail-Sicherheitslösungen, die verdächtige Nachrichten filtern.</i></p>
<p style="text-align: center;">Phishing-Tests</p> <p><i>Führen Sie regelmäßige Phishing-Simulationen durch, um die Wachsamkeit der Mitarbeiter zu erhöhen und Schwachstellen zu identifizieren.</i></p>	<p style="text-align: center;">Gerätemanagement</p> <p><i>Verwenden Sie Mobile Device Management (MDM) oder andere Lösungen, um alle Geräte im Homeoffice zu überwachen und zu verwalten.</i></p>	<p style="text-align: center;">Betriebssystem-Isolierung</p> <p><i>Nutzen Sie Virtualisierungs- oder Sandbox-Technologien, um Arbeitsumgebungen vom Hauptbetriebssystem zu isolieren.</i></p>
<p style="text-align: center;">Sicherheitsrichtlinien und -protokolle</p> <p><i>Stellen Sie sicher, dass alle Mitarbeiter die Sicherheitsrichtlinien und -protokolle kennen und befolgen.</i></p>	<p style="text-align: center;">Sicherheitsvorfälle und Reaktionspläne</p> <p><i>Erstellen und üben Sie Pläne für den Umgang mit Sicherheitsvorfällen, um schnell und effektiv reagieren zu können.</i></p>	<p style="text-align: center;">Rechtliche Anforderungen</p> <p><i>In vielen Ländern der EU ist die Ernennung eines Datenschutzbeauftragten durch die Datenschutz-Grundverordnung (DSGVO) vorgeschrieben, wenn Unternehmen bestimmte Kriterien erfüllen.</i></p>

2.2 ...und seien Sie auf den nächsten Cyberangriff vorbereitet.


Wenn bei Ihnen mehrere oder auch nur ein sicherheitsrelevanter Punkt nicht beachtet wurde, setzen Sie Ihr Unternehmen und all Ihre wertvollen Daten aufs Spiel!

Zögern Sie keine Sekunde länger – nehmen Sie sofort unseren umfassenden Sicherheits-Service in Anspruch, bevor es zu spät ist.

Ihre Sicherheit ist unsere höchste Priorität, und wir lassen nichts unversucht, um Sie zu schützen!"

3 Minimieren Sie deshalb Ihr Cyberrisiko und maximieren Sie Ihre IT-Sicherheit – Gerne, mit uns an Ihrer Seite

Im Folgenden sind kurz und **exemplarisch 30 von etwa 100** unseren Prüfschritten, Sicherheitskontrollen und daraus resultierenden Optimierungen aufgeführt.



profidata-IT | [Kontakt](#) | [Sensor-Daten](#) | [Recht und Orga](#) | [Internes](#)

Entscheidende IT-Sicherheits-Prüfungen, präzise Konfigurations-Tests und maximale System-Optimierungen!"

01

Betriebssystem-Updates:
Sicherstellen, dass das Betriebssystem auf dem neuesten Stand ist.

02

Antivirensoftware:
Installation und Aktualisierung von Antivirensoftware.

03

Firewall-Einstellungen:
Überprüfung und Konfiguration der Firewall.

04

Benutzerkonten:
Verwaltung und Sicherung von Benutzerkonten.

05

Festplattenplatz:
Überprüfung des verfügbaren Speicherplatzes.

06

Festplatten-Defragmentierung:
Regelmäßige Defragmentierung der Festplatte.

07

Datensicherung:
Einrichtung und Überprüfung regelmäßiger Backups.

08

Netzwerkverbindung:
Testen und Optimieren der Netzwerkverbindung.

09

Wi-Fi-Sicherheit:
Überprüfung und Konfiguration der Wi-Fi-Einstellungen.

10

Systemstart-Programme:
Verwaltung der Programme, die beim Start ausgeführt werden.

11

Leistungsüberwachung:
Überprüfung der Systemleistung und Ressourcen.

12

Treiber-Updates:
Sicherstellen, dass alle Gerätetreiber aktuell sind.

<p>13</p> <p>Druckereinstellungen: Konfiguration und Testen von Druckern.</p>	<p>14</p> <p>E-Mail-Client: Einrichtung und Optimierung des E-Mail-Clients.</p>
<p>15</p> <p>Cloud-Dienste: Integration und Verwaltung von Cloud-Diensten.</p>	<p>16</p> <p>Softwareinstallation: Installation und Aktualisierung notwendiger Software.</p>
<p>17</p> <p>Benutzerrechte: Verwaltung der Zugriffsrechte für verschiedene Benutzer.</p>	<p>18</p> <p>Internetbrowser: Überprüfung und Optimierung der Browser-Einstellungen.</p>
<p>19</p> <p>VPN-Einrichtung: Einrichtung und Testen von VPN-Diensten.</p>	<p>20</p> <p>Sicherheitszertifikate: Überprüfung und Erneuerung von Sicherheitszertifikaten.</p>

<p>21</p> <p>Proxy-Einstellungen: Konfiguration und Überprüfung der Proxy-Einstellungen.</p>	<p>22</p> <p>Remote-Zugriff: Einrichtung und Testen von Remote-Zugriffsmöglichkeiten.</p>
<p>23</p> <p>Daten-Verschlüsselung: Implementierung und Überprüfung von Verschlüsselungsmaßnahmen.</p>	<p>24</p> <p>Software-Lizenzen: Überprüfung und Verwaltung von Softwarelizenzen.</p>
<p>25</p> <p>Benachrichtigungssysteme: Einrichtung von Systemen zur Überwachung und Benachrichtigung.</p>	<p>26</p> <p>Patch-Management: Verwaltung und Anwendung von Software-Patches.</p>

<p>27</p> <p>Passwort-Management: Einrichtung und Überprüfung eines Passwortmanagers.</p>	<p>28</p> <p>System-Bereinigung: Entfernung unnötiger Dateien und Programme.</p>
<p>29</p> <p>App-Konfiguration: Optimierung der Einstellungen installierter Anwendungen.</p>	<p>30</p> <p>Mobile Geräte: Verwaltung und Sicherheit mobiler Geräte, die mit dem Netzwerk verbunden sind.</p>

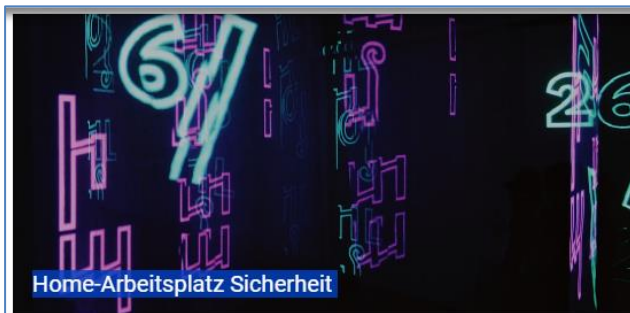
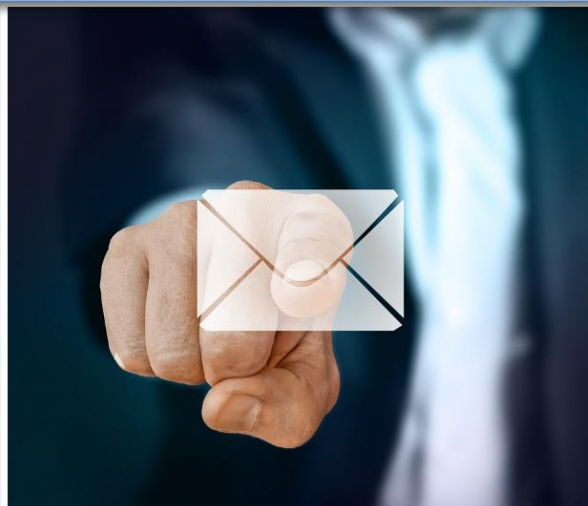
4 Maximale Sicherheit, minimaler Stress – perfekt geschützt!



HOME-ARBEITSPLATZ SICHERHEIT

Wir prüfen und optimieren die Sicherheit im Home-Office und Ihrem Heim-Netzwerk...

Die Notwendigkeit der Maßnahmen ist klar und dringlich.
Jede Verzögerung könnte Ihre Sicherheit gefährden und unnötige Risiken verursachen.
Werden Sie jetzt aktiv und sichern Sie sich unsere Unterstützung, bevor es zu spät ist!

Fordern Sie IT-Sicherheit für Ihren Arbeitsplatz an...

Ihr Name oder ihr Unternehmen
Bitte Ihren Namen oder Firma oder Unternehmen angeben...

Ihre E-Mail für unsere Rückmeldungen
Bitte Ihre E-Mail-Adresse eintragen...

Betrifft die Sicherheit im Home-Office und IT-Arbeitsplatz
Fordern Sie uns an – oder beschreiben kurz Ihr Anliegen...

ABSENDEN / ANFORDERN...