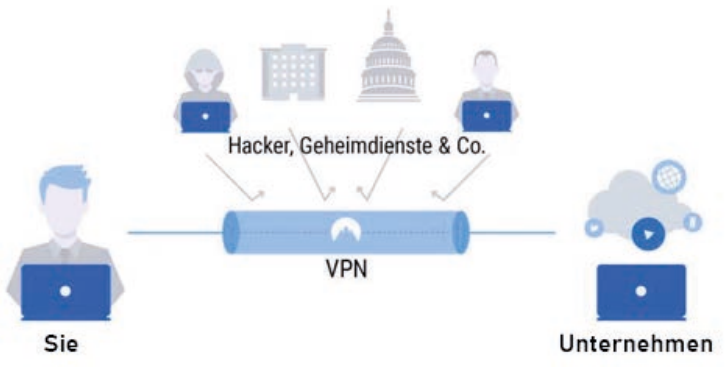
10 Punkte Maßnahmenplan für ein sicheres Home Office

10 Punkte, die zu beachten sind, wenn Mitarbeiter aufgrund der aktuellen Ausnahmesituation aus dem „Home Office“ arbeiten müssen.

1. Prüfen Sie, in wie weit eine sinnvolle Kommunikation mit dem Mitarbeiter und den Kollegen im Unternehmen möglich ist. Hier gilt es z.B. auch die Möglichkeiten der Telefonanlage zu prüfen. Nicht immer können bestimmte Rufnummern wie z.B. Support Hotline o.ä. auf andere Telefone umgeleitet werden!

Sollte es hier zu möglichen Herausforderungen kommen, kann man kurzfristig an Lösungen arbeiten.

2. In jedem Fall gilt: der Zugang zum Unternehmensnetzwerk muss sich so sicher wie möglich gestalten und sollte nur über eine dedizierte Client/ VPN Verbindung und einer 2 Faktor Authentifizierung oder Zertifikate erfolgen.



Persönlichen Ansprechpartner erreichen:

THE BRISTOL GROUP Deutschland GmbH
Robert-Bosch-Straße 13
63225 Langen
Per E-Mail an: anfragen@bristol.de

3. Prüfen Sie im Zusammenhang mit VPN unbedingt, ob für das VPN Gateway ausreichend Lizenzen zur Verfügung stehen und ob das VPN Gateway für solch ein erhöhtes Aufkommen an VPN Verbindungen über genügend Leistung verfügt.

Sollte es hier zu Problemen bzw. Ausfällen kommen, können wir innerhalb kürzester Zeit mit Ihnen Lösungen erarbeiten und zur Verfügung stellen.

4. Am besten und vor allem am sichersten arbeiten Mitarbeiter aus dem Homeoffice, wenn sie das Arbeitsgerät vom Unternehmen zur Verfügung gestellt bekommen. Je nach Aufgabengebiet reicht hier ggf. ein Tablet oder basierend auf die Anforderung ein Notebook. Auf den vom Unternehmen zur Verfügung gestellten Geräten können alle für die Verbindung ins Unternehmen benötigten Tools bereits installiert sein, was insbesondere auch für die entsprechenden Sicherheitskomponenten gilt (AV-, ABot-, Ransomware Protection usw.).

5. Sollte Punkt 4. aus Gründen der Verfügbarkeit von entsprechenden Systemen nicht gegeben sein, kann auch darüber nachgedacht werden, ob die Mitarbeiter von vorhandenen, eigenen Systemen arbeiten können. Da Sie hier nie sicher sein können, wer noch an dem PC arbeitet und wie sich an diesen Systemen die Sicherheit gestaltet, muß der Zugang zum Unternehmen besonders betrachtet werden.

6. Für die Punkte 4. und 5. gilt letztendlich, dass Sie die Umgebung nicht kennen, in der entweder das unternehmenseigene System oder das Mitarbeiter eigene System betrieben wird. Diese Herausforderung wirft weitere Fragen auf, die es zu klären gilt:

- Gibt es Drucker im privaten Bereich? Ist die Möglichkeit zum Ausdruck erwünscht oder nicht?
- Muss das PC-System während der Home-Officezeit auch von anderen Familienmitgliedern verwendet werden?

In diesem Fall sollte man von diesem Arbeitsplatz keinerlei Verbindungen ins Unternehmen zuzulassen, sondern ein Unternehmensgerät zur Verfügung stellen.

7. Für den VPN-Zugang müssen Zertifikate verwendet werden, die in entsprechenden USB-Zertifikats Speichern abgelegt sind. Damit wird verhindert, dass Mitarbeiter diese von einem USB Stick auf den Desktop des Arbeitsplatzes kopieren und damit die zusätzliche Sicherheit unwirksam wird.

Sollte dies nicht möglich sein, so muß zumindest eine 2-Faktor Authentisierung eingerichtet werden. Der Mitarbeiter erhält dann beim Aufbau der Verbindung nach Eingabe seines Passwortes z.B. einen 2. Key an sein Smartphone geschickt, mit dem die Verbindung vervollständigt wird. Alternativ gibt es Soft- oder Hardwaretokens von Fortinet, RSA oder anderen Anbietern, die eine Nummer anzeigen, die zusätzlich zum Passwort eingegeben werden muß.

8.: Sobald nun die Mitarbeiter über das firmeneigene- oder das private Gerät einen VPN Tunnel gestartet haben, ist das einzige Werkzeug, das verwendet werden kann, ein Terminal Client. Dieser kann entweder mit Bordmitteln von Windows bereitgestellt werden oder es können selbstverständlich auch andere Hersteller verwendet werden (Cisco, Citrix usw.) Diese Terminal Clients sollten derart konfiguriert werden, dass aus diesen maximal auf einen vorhandenen Drucker gedruckt werden kann, wenn erforderlich. Ansonsten sollte der Client so eingestellt sein, dass kein Datei-Export oder -import von und zu dem verwendeten PC erfolgen kann.

Auch diese Faktoren sollten bei der Vergabe von Heimarbeitsplätzen, auch in Krisenzeiten berücksichtigt werden.

9.: Statten Sie die eigenen Geräte, die Sie Ihren Mitarbeitern übergeben mit Bildschirmfiltern aus, mit denen ein seitlicher Einblick auf den Bildschirm erschwert wird. Mitarbeiter, die eigene Geräte verwenden, sollte auferlegt werden, derartige Filter zu verwenden, damit unberechtigte Personen möglichst keinen Einblick in ggf. vertrauliche Daten erhalten.

10.: Eine praktikable Vorgehensweise wäre, sich ein Bild des jeweiligen Arbeitsplatzes zu machen. Nur damit ließe sich vorab einschätzen, ob der Mitarbeiter überhaupt in der Lage ist, seiner Arbeit zuhause nachzukommen. In der Regel wird es dafür keinen separaten Raum geben, ggf. sind weitere Familienmitglieder anwesend oder Haustiere. Letztere können bei Telefonaten störend wirken, während weitere Familienmitglieder am Bildschirm Dinge mitbekommen, die vertraulich sind oder aber bei Telefonaten Informationen aufschnappen und weitererzählen, die ebenfalls vertraulich und für Dritte nicht bestimmt sind.

Haben Sie weitere Fragen zur sicheren Umsetzung einer Home Office Lösung oder allgemein zum Thema IT-Sicherheit? Unsere IT-Security Experten stehen Ihnen gerne persönlich mit Rat und Tat zur Seite.

Kennen Sie schon unseren BonD Call – BRISTOL on Demand ? 24/7 IT-Securtiy Service auf Abruf!*

Wir unterstützen Sie gerne mit telefonischem Support. Ob im Notfall oder begleitend bei Ihrer Systemumstellung. Egal ob Sie außerhalb Ihrer Wartungszeiten Unterstützung benötigen, oder Ihr Dienstleister die Lösung nicht findet. Sprechen Sie uns an!

*Leistung außerhalb der Geschäftszeiten nicht garantiert.

THE BRISTOL GROUP - unsere Standorte:

Zentrale Rhein Main
Robert-Bosch-Straße 13
63225 Langen
Tel.:06103 - 20 55 300
Fax: 06103 - 70 27 87

Standort München
Dieselstraße 25
85748 Garching
Tel.: +49 (0)89 - 36 03 45 47 0
Fax: +49 (0) 89 / 36 03 45 47 7

Niederlassung Berlin
Uhlandstraße 181 - 183
10623 Berlin
Tel +49 (0) 30 – 31 00 76 10
Fax +49 (0) 30 – 31 00 7620

IT-Security Support/Beratung erhalten Sie hier:

www.bristol.de
anfragen@bristol.de