UMSTELLUNG HOME-OFFICE

EINE ANLEITUNG FÜR KLEINE UND MITTELSTÄNDISCHE UNTERNEHMENEN

Whitepaper Version 1.0 | März 2020 | Autor: Hannes Hartung

Vorbemerkung

In Zeiten der Digitalisierung wird Mitarbeitenden zunehmend die Option gewährt, Arbeiten aus dem heimischen Büro zu erledigen. Gerade für Aufgaben, welche in Ruhe erledigt werden müssen, ist das Großraumbüro nicht die beste Option. Weiterhin wünschen sich viele Angestellte mehr Flexibilität im Rahmen ihres Arbeitsverhältnisses und somit wird Home-Office zunehmend an Tragweite gewinnen. Darüberhinaus hat die derzeitige Coronakrise gezeigt, dass Unternehmen in der Lage sein müssen, remote gut zusammenzuarbeiten. Somit lohnt es sich für alle Firmen vorzusorgen und Rahmenbedingungen zu schaffen. Da die Infrastruktur und die allgemeinen Rahmenbedingungen im Home-Office nicht dieselben wie im Firmenbüro sind, gilt es sich im Bereich der IT-Sicherheit abzusichern, um kein Einfallstor für Cyberangriffe zu liefern.

Dieses Whitepaper soll einen groben Überblick über die notwendigsten Maßnahmen geben. Um ein aadäquates IT-Sicherheitsniveau im Home-Office sicherzustellen, ist der Arbeitgeber in der Pflicht die nötigen Rahmenbedingungen zu schaffen. Aus diesem Grund sollten Checklisten und Richtlinien kommuniziert werden, um den Mitarbeitenden eine sinnvolle Struktur vorzugeben. Gerade im Hinblick auf die zu verwendenden Kollaborationsanwendungen zur Kommunikation im Team sollten gesonderte Regelungen getroffen und kommuniziert werden.

Festplattenverschlüsselung für mobile Arbeitsgeräte

Um Daten beim Verlust oder Diebstahl von mobilen Endgeräten zu sichern, ist eine Festplattenverschlüsselung zwingend notwendig. Die Festplattenverschlüsselung sollte für die gesamte Festplatte oder zumindest einzelne Partitionen aktiviert werden. Ist die komplette Festplatte vollverschlüsselt, muss vor dem booten der Authentifizierungsmechanismus erfüllt werden (Passwort oder Hardware). Als Verschlüsselungsverfahren kommt häufig der Advanced Encryption Standard (AES) zum Einsatz, der in seiner neuesten Form als sicher gilt. Durch die Verschlüsselung von Dateinamen sind Rückschlüsse auf den Inhalt nicht möglich. Der Vorteil der Festplattenverschlüsselung ist, dass das Auslesen der Festplatten ohne Schlüssel nicht mehr möglich ist. Somit kann die Festplatte auch nicht von Angreifern ausgebaut und an einem anderen Rechner entschlüsselt werden, wenn der Schlüssel nicht vorhanden ist. Unter Umständen kann von Nachteil sein, dass die Performance aufgrund der Ver- und Entschlüsselung mit zunehmender Datenmenge etwas beeinträchtigt ist, und weiterhin darf der Schlüssel nicht verloren gehen, da sonst in aller Regel die Daten unwiederbringlich verloren sind. Für einige Windows-Versionen ist das Programm BitLocker erhältlich und kann ohne Probleme aktiviert werden. Für MacOS-Geräte existiert das bereits bei Auslieferung integrierte Tool FileVault. Weitergehend existieren betriebssystemübergreifende Open-Source-Lösungen, welche eingesetzt werden können, z.B. VeraCrypt. Für die verschiedenen Werkzeuge existieren leicht verständliche Anleitungen zur Einrichtung.

VPN – Virtual Private Network

Dringend empfohlen wird die Einrichtung eines VPN-Zuganges. Dieser stellt eine verschlüsselte Übertragung von Daten über öffentliche Netze, wie das Internet, sicher. Dabei bietet der VPN die Möglichkeit, auf ein vorhandenes Netzwerk von außen sicher zuzugreifen. Wie funktioniert das Ganze? Einen VPN-Tunnel kann man sich sozusagen wie einen echten Autobahntunnel vorstellen. Die Datenpakete werden zwischen den VPN-Teilnehmern verschlüsselt übertragen und sind somit für Außenstehende, in verschlüsselter Form, unlesbar. Man spricht deshalb auch von einem „VPN-Tunnel“.

Eine Open-Source-Lösung, um ein VPN aufzubauen, ist z. B. OpenVPN. Zur Verschlüsselung kann SSL oder mbed TLS und für den Transport UDP oder TCP benutzt werden. Eine Anleitung zur Einrichtung sowohl von VPN-Clients als auch VPN-Servern mit OpenVPN findet sich hier: https://openvpn.net/vpn-server-resources/#guides.

Eine Empfehlung für eine Lösung zu geben, ist nicht zielführend. Da die Auswahl an die verschiedenen Anforderungen geknüpft ist. Es existieren ebenso kommerzielle Lösungen, und die Unterschiede der Kosten, Performance und Features sind groß. Einen umfassenden Überblick über Möglichkeiten bietet folgende Webseite: https://thatoneprivacysite.net/.

E-Mail-Verschlüsselung

Die Einrichtung eines Verfahrens zum ver- und entschlüsseln von E-Mails gehört auch im normalen Office-Betrieb zum Pflichtprogramm. Eine E-Mail ist vergleichbar mit einer Postkarte und sollte dementsprechend vor der Kenntnisnahme unbefugter Dritter geschützt werden. Derzeit haben sich in der Praxis vor allem die Verfahren SMIME und PGP/MIME durchgesetzt. Das Verfahren PGP/MIME kann kostenfrei unter Windows durch gpg4win (https://www.gpg4win.de/) implementiert werden.

Für eine Anleitung zur Einrichtung können Sie uns jederzeit kontaktieren.

Zutrittssicherheit

Gerade in Wohngemeinschaften oder Mehrpersonenhaushalten muss auch die Einsichtnahme in Daten, sowohl digital als auch analog, geregelt werden. Aus diesem Grund sollte der heimische Arbeitsplatz abschließbar sein und verschließbare Schränke enthalten.

Absicherung von Drucker- und Multifunktionsgeräten

Gerade die Absicherung von Multifunktionsgeräten und Druckern wird unterschätzt. Die meisten Haushalte haben heutzutage ein Multifunktionsgerät, welches über WLAN mit dem Privatnetzwerk verbunden ist. Am sinnvollsten ist die Besorgung eines günstigen Zweitgerätes, welches nur für den Heimarbeitsplatz zur Verfügung steht. Wenn mehrere Personen im Haushalt auf ein und denselben Drucker zugreifen, ist es schwieriger die geforderten Sicherheitsmaßnahmen sicherzustellen. Um erhöhte Sicherheitsaufwände zu vermeiden, sollte das Zweitgerät über LAN mit dem Arbeitsplatzrechner verbunden werden und nur für Geschäftliches genutzt werden.

Protokollierung und Analyse von Ereignissen

Jegliche Remote-Aktivitäten sollten den entsprechenden Usern zugeordnet werden und jegliche Anomalien mit Sicherheitstools, z. B. SIEM/UEBA, überwacht werden. Um im Home-Office produktiv arbeiten zu können, ist es notwendig Daten auf Rechner/Laufwerke herunterzuladen. Die Protokolle von den wichtigsten Exfiltrationspunkten wie z. B. VPN, Office 365 sollten überwacht und analysiert werden, um mögliche Datenschutzverletzungen frühzeitig zu erkennen. Achten Sie vor allem bei der Überwachung der Zugriffsberechtigungen auf Auffälligkeiten, wie z. B.:

- die Nutzung abgelaufener Userkonten, welche nach wie vor aktiv sind,
- unlogische Ausweitung von Berechtigungen,
- Nutzung von stillgelegten Userkonten.

Weiterhin sollte die unberechtigte Weitergabe von Zugriffsberechtigungen mit einer Richtlinie geregelt und Verstöße sanktioniert werden. Häufig werden langwierige Freigabeprozesse durch die Weitergabe von Zugriffsberechtigungen umgangen. Auffälligkeiten für solche Verstöße sind u. A.:

- User, welche gleichzeitig von mehreren Standorten Anmeldeversuche starten,
- User, welche angemeldet sind und sich versuchen remote anzumelden.

Multi-Faktor-Authentifizierung

Es sollte darauf geachtet werden, für alle Anwendungen, falls möglich, eine Multi-Faktor-Authentifizierung einzurichten, um die Sicherheit zu erhöhen. Gerade der Zugriff der Mitarbeitenden auf Sharepoint, GoogleDrive und Co sollte durch Multi-Faktor-Authentifizierung abgesichert werden.

Schutz vor Social Engineering

Gerade Social Engineering wird durch die steigende Anzahl an Mitarbeitenden im heimischen Büro von Kriminellen vermehrt genutzt. Bei Social Engineering handelt es sich um die Manipulation von Menschen, um an sensible Informationen zu gelangen. Um sich davor zu schützen, sollten seitens der Geschäftsführung ganz klare Verantwortlichkeiten und Freigaben erteilt werden. Zusätzlich müssen Mitarbeitende sensibilisiert werden, um Awareness zu schaffen.

Zusammenfassung:

Zusammenfassend kann man sagen, dass folgende Mindeststandards eingehalten werden sollten:

- Der Heimarbeitsplatz sollte abtrennbar und in einem abschließbaren Raum sein.
- Die IT-Ausstattung sollte möglichst vom Arbeitgeber gestellt werden.
- Festplatten und Datenträger sollten mit einem Verschlüsselungsverfahren nach Stand der Technik abgesichert werden.
- Firewalls und andere Schutzmaßnahmen des Unternehmens müssen auch im Home-Office gelten, wenn eine Einwahl ins Unternehmens-Netzwerk vorgesehen ist.
- Der Netzwerkzugriff sollte über einen VPN-Tunnel abgesichert sein.