HOME-OFFICE-GUIDE FÜR KMU

Das Home-Office wurde in der Pandemie für Viele von heute auf morgen fast selbstverständlich. Im Rückblick wissen wir, dass die Sicherheit dabei oft auf der Strecke geblieben ist – wie sollte es auch anders gehen in der Kürze der Zeit?
Spätestens jetzt ist es an der Zeit, das zu ändern!

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

DIGITAL SICHER NRW

WIE SCHÜTZE ICH MEIN UNTERNEHMEN ZUHAUSE?

JETZT HANDELN - KRIMINELLE SIND UNS EINEN SCHRITT VORAUS.

Viele Unternehmen – ganze 58% – haben in einer Studie des Bundesamts für Sicherheit in der Informationstechnik angegeben, dass sie das Home-Office auch nach der Pandemie beibehalten oder sogar erweitern wollen.
Dabei sind Cyberkriminelle längt einen Schritt weiter: Das Home-Office ist zu einem bevorzugten Einfallstor für Hacks, Erpressungen und Virenbefall geworden. Schützen Sie ihr Unternehmen und nehmen Sie die dringend notwendigen Sicherheitsmaßnahmen in Angriff – jetzt!

IT-SICHERHEIT IST TEAMWORK.

Der Knackpunkt bei der Sicherheit im Home-Office ist, dass Geschäftsführung, IT-Verantwortliche und Mitarbeiterinnen und Mitarbeiter an einem Strang ziehen müssen – nur, wenn jeder und jede Ihren Teil beiträgt, lässt sich eine sichere Infrastruktur aufbauen.

WIR ZEIGEN IHNEN DIE BASICS.

Je nach Branche und Art der Daten müssen - wie im Betrieb auch – unterschiedlich hohe Sicherheitsvorkehrungen getroffen werden. Ein paar grundlegende Maßnahmen sollten Sie allerdings in jedem Fall treffen. Diese zeigen wir Ihnen hier.

DIGITAL SICHER NRW

HOME-OFFICE – BASICS FÜR ALLE MITARBEITENDE

1. EINE VERTRAULICHE ARBEITSUMGEBUNG SCHAFFEN

Sorgen Sie dafür, **dass Telefonate und sensible Unternehmens-daten auch im Home-Office vertraulich bleiben.** Stellen Sie sicher, dass weder Ihre Nachbarn, noch Passanten oder Besuch mithören oder mitlesen, was Sie auf der Arbeit tun.

Wichtige Meetings sollten Sie deshalb auch nicht im Garten oder auf dem Balkon durchführen. Schließen Sie im Zweifelsfall die Fenster.

2. SICHT- UND ZUGRIFFSSCHUTZ NUTZEN

Nutzen Sie sogenannte **"Blickschutzfolien"** auf Laptops, Tablets und Handys, die dafür sorgen, dass niemand von der Seite auf Ihren Bildschirm schauen kann. **Sperren Sie außerdem Ihren Rechner**, wenn Sie Ihren Arbeitsplatz verlassen.

Unter Windows geht das mit der Tastenkombination **WINDOWSTASTE+L**, den Mac sperren Sie mit **COMMAND+CONTROL+Q**.

3. RICHTEN SIE EINE MEHR-FAKTOR-AUTHENTISIERUNG EIN

Das Prinzip der "MFA" kennen Sie bereits vom Online-Banking – wenn Sie sich einloggen, müssen Sie einen Code eingeben, der auf Ihr Smartphone oder ein anderes Gerät geschickt wird. So sind sie doppelt sicher, wenn jemand Ihr Passwort gestohlen hat: Ohne den zweiten Code auf Ihrem Smartphone, bekommen Fremde keinen Zugriff auf Ihre Daten.

Die MFA können Sie selbst einrichten: *Stellen Sie in den Einstellungen Ihres Dienstes die MFA an und legen Sie fest, auf welches Gerät Sie den Code erhalten wollen. Fertig!*

4. FÜHREN SIE REGELMÄSSIGE SICHERHEITSUPDATES BEI IHRER GESAMTEN SOFTWARE DURCH.

Softwarehersteller machen Updates nicht um Sie zu ärgern, sondern schließen damit Schwachstellen und Sicherheitslücken, damit Kriminelle nicht in ihr System hineingelangen können. **Geupdatet werden muss deshalb nicht nur der Virenscanner, sondern alle Programme, die Sie nutzen.**

Stellen Sie ein, **dass Updates automatisch durchgeführt werden**. Erinnern Sie in der Firma regelmäßig an Updates – in einigen Unternehmen gibt es dafür sogar feste Zeitfenster.

DIGITAL SICHER NRW

HOME-OFFICE – BASICS FÜR IT-VERANWORTLICHE

Ziehen Sie im Zweifelsfall ein Dienstleistungsunternehmen heran, dass Sie bei der Einrichtung unterstützt!

5. RICHTEN SIE EIN VIRTUAL PRIVATE NETWORK EIN

Ein virtuelles privates Netzwerk (**VPN**) ist eine **Netzwerkverbindung, die Sie vor der Einsicht von Unbeteiligten schützt und Ihr Kommunikationsnetz nach außen abschirmt.** Die Mitarbeiterinnen und Mitarbeiter loggen sich von Zuhause in dieses Netz ein wie auch diejenigen, die im Betrieb vor Ort arbeiten.

Dieses Netz lässt sich von zentraler Stelle aus besonders schützen, etwa indem man dessen Datenverkehr verschlüsselt.

6. NUTZEN SIE EIN MOBILE DEVICE MANAGEMENT

Mobile Device Management (deutsch: Mobilgeräteverwaltung) bedeutet, dass Sie mobile Geräte wie Laptops, Tablets und Smartphones an zentraler Stelle verwalten können. Als Admin können Sie durch die drahtlose Verwaltung der Geräte bestimmte Einstellungen vornehmen, automatische Aktualisierungen einspielen und das Gerät sperren, sollte es einmal verloren gehen.

Die Fernverwaltung lässt sich mit Hilfe einer Software organisieren und bei Bedarf auch vollständig automatisieren.

7. VERSCHLÜSSELN SIE ENDGERÄTE UND DATENTRÄGER

Alle Geräte und Datenträger, die an an die Mitarbeitenden ausgegeben werden, sollten verschlüsselt werden. Denn dann können die Daten nicht vom Dritten gegen Sie verwendet werden, wollte ein Gerät mal verloren gehen. Technisch können Sie dafür beispielsweise die Verschlüsselung nutzen, die in den Betriebssystemen schon integriert ist.

Das ist "Bitlocker" unter Windows und "Fire-Vault" beim Mac. Darüber hinaus gibt es verschiedene kostenfreie und kostenpflichtige Programme, die zusätzlich verwendet werden können, z.B. VeraCrypt.

DIGITAL SICHER NRW

DER SCHLÜSSEL ZUM SICHEREN HOME-OFFICE IST DIE GESCHÄFTSFÜHRUNG

ALLE SIND GEFRAGT: ANGEFANGEN BEI DER GESCHÄFTSFÜHRUNG

Gerade im Home-Office sind in Sachen Sicherheit nicht mehr allein die IT-Abteilung oder die IT-Verantwortlichen gefragt. Viel stärker noch als im Betrieb tragen die Mitarbeiterinnen und Mitarbeiter die Verantwortung dafür, dass die IT-Infrastruktur keine Angriffsflächen bietet.

Die Sicherheit im Home-Office steht steht auf den Schultern der

- **IT-Sicherheitskompetenz Ihrer Mitarbeitende,**
- **der von IT-Admins eingerichteten Infrastruktur,**
- **der Bedeutung, die die Geschäftsführung dem Thema beimisst.**

Nur die Führungsebene kann dem Thema die Bedeutung geben, die es angesichts der aktuellen Gefahrenlage benötigt. Sie muss dafür sorgen, dass das Thema im Betrieb ernst genommen wird und dass Zeit und Ressourcen zur Verfügung stehen.

Sorgen Sie als Geschäftsführende dafür, dass die wichtigsten Maßnahmen von Ihren IT-Verantwortlichen oder Ihrem Dienstleistungsunternehmen umgesetzt werden. Schaffen Sie verbindliche IT-Sicherheitsregelungen und schicken Sie Ihre Angestellten regelmäßig zu Schulungen.

Machen Sie regelmäßig darauf aufmerksam, dass IT-Sicherheit in der digitalen Welt dazugehört!

Kostenlose Schulungsangebote und weitere Informationen finden Sie auf **www.digital-sicher.nrw**.

HOME-OFFICE – BASICS FÜR DIE CHEF-ETAGE

DIGITAL SICHER NRW

8. STELLEN SIE DAS THEMA IN DEN VORDERGRUND

Mitarbeiterinnen und Mitarbeitern ist oft nicht bewusst, dass gerade kleine und mittlere Unternehmen vielleicht sogar um ihre Existenz fürchten müssen, wenn sie ein Cyberangriff trifft. Als Geschäftsführung sind Sie gefragt, Ihre Angestellten zu sensibilisieren, über die Risiken aufzuklären und Ihnen Schutzmaßnahmen zu zeigen.

Machen Sie in Teamsitzungen auf das Thema aufmerksam, erläutern Sie die Gefahrenlage und erinnern Sie Ihre Angestellten regelmäßig an die wichtigsten Maßnahmen.

9. SCHAFFEN SIE VERBINDLICHE IT- SICHERHEITSREGELUNGEN FÜR DAS HOME-OFFICE

Für eine sichere Arbeit zuhause sollten Sie eine verbindliche Sicherheitsregelung schaffen, auf die sich alle Mitarbeitenden verpflichten. Halten Sie diese Regelung als schriftliche Vereinbarung fest, die von allen Mitarbeiterinnen und Mitarbeitern unterzeichnet wird.

Hier können Sie verabreden, wie Geräte aufbewahrt werden, welche Netzwerk-verbindungen genutzt werden sollten, welche Art Passwort für den Zugriff auf welche Dienste verwendet werden soll, was im Notfall zu tun ist und Vieles mehr.

10. SCHULEN SIE REGELMÄSSIG IHRE ANGESTELLTEN

Ohne Ihre Mitarbeiterinnen und Mitarbeiter geht es nicht – klären Sie deshalb mit Schulungen regelmäßig über die Gefahren, Vorsichtsmaßnahmen und Verhaltensregeln auf.

Kostenlose Schulungsangebote finden Sie auf www.digital-sicher.nrw.