Von **zu Hause** arbeiten

Für das Home-Office hat die IT-Sicherheit oberste Priorität. DANIEL MARKUSON hat dazu die folgenden Tips ...

Das absolute Minimum ist der Paßwortschutz des Routers, um das Heimnetzwerk abzusichern, falls noch nicht vorhanden. Dazu kommen diese zusätzlichen Maßnahmen:

- SSID-Übertragungen ausschalten. Dies macht es schwieriger, das heimische WLAN-Netzwerk zu finden (für alle, die es nicht finden sollen);
- MAC-Adressen filtern. Eine MAC-Adresse ist ein Netzwerkname, der einem bestimmten Gerät zugeordnet ist. Falls ein Router das Filtern von MAC-Adressen unterstützt, wird es gleich um ein Vielfaches schwieriger für unautorisierte Geräte, sich mit dem Router zu verbinden.
- Ein Gastnetzwerk einrichten. Ein Gastnetzwerk ist ein zweites Netzwerk, das man auf seinem Router einrichten kann – speziell für die Geräte von Gästen. Abhängig vom Router können beiden Netzwerke auch mit verschieden Sicherheitsregeln versehen werden. In diesem Fall ist es ratsam, sowohl die privaten, als auch die Arbeitsgeräte hinter den strengsten Sicherheitsregeln zu schützen, und weniger strikte Einstellungen für das Gastnetzwerk zu verwenden.
- Ein VPN auf dem Router installieren. Falls auf dem Router angemessene Verschlüsselung eingestellt ist, sollte man auch ein VPN auf dem Router einrichten. Dieses hat einzigartige Vorteile und Nachteile.

Ein anderes Gerät oder Account für die Arbeit benutzen

Am besten ist es, persönliche und berufliche Geräte zu trennen. Auf diese Weise bleibt das eine sicher, falls das andere eine Sicherheitslücke aufweist. Arbeit, die man am PC erledigen kann, läßt sich zumeist auch am Laptop erledigen. Dies ist die beste Alternative, da dieser schon alle Sicherheitstools hat, die die Firma bereitstellt.

Alternativ kann man auch einfach einen separaten Benutzeraccount auf seinem privaten Gerät benutzen. Allerdings muß man dann darauf achten, alle Apps zu haben, die man benötigt, um sicher und geschützt zu arbeiten. Falls man sich fast nie in diesen Account einloggt, ist es essentiell, alle Softwareupdates durchzuführen, bevor man anfängt zu arbeiten. Ältere Versionen könnten inkompatibel mit der Software von Kollegen sein, und auch wichtige Sicherheitsupdates könnten unter Umständen nicht mehr bereitgestellt werden.

Firmeninterne Online-Sicherheits-Software nutzen

Es gibt viele verschiedene Programme, die den Mitarbeitern das Arbeiten von zu Hause erleichtern können. Einige der einfachsten und effektivsten sind NordVPN Teams oder NordVPNs Dedicated IP für Einzelpersonen. So funktionieren sie:

- Die Firma erstellt eine sogenannte “Whitelist” für alle ihre Server und Systeme. Eine Whitelist funktioniert wie ein Türsteher vor einem Club – wenn deine IP nicht auf der Liste steht, kommst du nicht rein.
- Mit NordVPN Teams oder Dedicated IP kann man seine IP-Adresse in eine der zugelassenen IP-Adressen ändern. Dies kann man von überall in der Welt machen, und damit verschlüsselten Zugang to Servern und Systemen bekommen, die man andernfalls nur aus dem Büro selbst abrufen

>>

kann. Es existieren noch viele weitere Lösungen. Persönliche Tools wie sichere Browser und Browser-Extensions bis hin zu sicheren Messaging-Apps helfen allen, ihren Alltag sicher zu gestalten. Bevor man das Büro verläßt und sein gemütliches Home Office einrichtet, sollte man den Systemadministrator zu Rate ziehen, ob es Programme gibt, die man zunächst noch installieren sollte.

Sensible Dateien für Transfer und Speicherung verschlüsseln

Die zentralen Firmenserver und -netzwerke sind hoffentlich geschützt, aber wenn viele Mitarbeiter von zu Hause arbeiten, kann so einiges passieren.

Glücklicherweise gibt es Tools, die die Verschlüsselung von Dateien sowohl in der Speicherung, als auch im Transfer erlauben. Egal von wo man arbeitet oder Dateien versendet, werden diese mit NordLokker sicher verschlüsselt. Durch die Verknüpfung der Accounts von allen Kollegen wird eine Ende-zu-Ende-Verschlüsselung garantiert – die beste Sicherheit für die sensibelsten Daten. Das Beste daran ist, daß NordLocker KOSTENLOS für die ersten 2GB ist.

Über Cybersecurity und Social Engineering informiert bleiben

Um zu wissen, worauf man achten muß, sollte man über die verschiedenen Formen von Social Engineering und Phishing Bescheid wissen. So versuchen Betrüger, sich als Kollegen oder Manager auszugeben, um an sensible Firmeninformationen zu gelangen. Zu den genannten Tools gibt es viele Informationen, aber hier einige Basics:

Den Absender überprüfen. Wurde die Chatnachricht vom Boss gerade von John.Doe oder von John_Doe geschickt? Welcher ist richtig? War die E-Mail mit dem angeblich so wichtigen Anhang von *john.doe@deinefirma.de* oder von *john.doe@fastdeinefirma.de*.

Nichts runterladen oder anklicken, bis man sicher sein kann, daß der Absender echt ist. Selbst dann kann es sinnvoll sein, kurz bei dem betreffenden Kollegen nachzufragen, insbesondere, wenn es um sensible Daten oder zum Beispiel Geldtransfers geht.

Zweite Kommunikationsmöglichkeiten nutzen. Falls man sich über die korrekte Schreibweise eines Accounts seines Kollegen unsicher ist, sollte man lieber anrufen, um nachzufragen. Falls man gerade kurz davor ist, etwas aus der E-Mail eines Kollegen herunterzuladen, sollte man ihn oder sie vielleicht zuerst kurz im Chat anschreiben. So ist es viel schwieriger für Fakenachrichten, Schaden anzurichten.

Öffentliches W-LAN vermeiden

Öffentliches W-LAN ist immer eine Gefahr, weil es viel weniger sicher ist als ein privates W-LAN und die Wahrscheinlichkeit von damit verbundenen Betrügern viel höher. Doch W-LAN-Netzwerke sind nicht die einzige Gefahr in der Öffentlichkeit. Hier sind nur ein paar der weiteren Gefahren, die bei der Arbeit in der Öffentlichkeit lauern können.

USB Ladegeräte. Normalerweise sind USB Ladegeräte nur Ladegeräte. Manchmal können öffentliche Zugänge allerdings mit Hardware oder Software ausgestattet oder gehackt sein und so Malware auf dem ladenden Gerät installieren oder die Kommunikation mitlesen. Daher sollte man besser auf seine Geräte zu Hause vertrauen.

Mithörer. Wenn man normalerweise im Büro arbeitet, ist man daran gewöhnt, manchmal auch sensible oder vertrauliche Themen offen zu besprechen. In der Öffentlichkeit können so allerdings Informationen ganz leicht in die falschen Hände geraten. Dieses Risiko kann vermieden werden, indem man alleine zu Hause arbeitet oder umgeben von Leuten, denen man vertraut.

Noch Fragen?
https://nordvpn.com

IMPRESSUM

Computern im Handwerk/ handwerke.de
gegründet 1984, dient als unabhängiges Fachmagazin für moderne Kommunikation den Betrieben der **Bauhaupt- und Nebengewerbe** im „portionierten" Wissens- und Technologie-Transfer.

Herausgeber: Horst Neureuther

CV Computern-Verlags GmbH
Goethestraße 41, 80336 München

Telefon o 89/54 46 56-0
Telefax o 89/54 46 56-50
Postfach 15 06 05, 80044 München
E-Mail: info@cv-verlag.de
redaktion@cv-verlag.de
www.handwerke.de

Geschäftsleitung:
Dipl.-Vw. H. Tschinkel-Neureuther

Anzeigenleitung:
Dipl.-Vw. Heide Tschinkel-Neureuther
e-mail: anzeigen@cv-verlag.de

Redaktion und redaktionelle Mitarbeiter in dieser Ausgabe:
Markus Bernhart, Jens Kathmann, Margrit Lingner, Björn Lorenz, Andreas G. Mantler, Daniel Markuson, Horst Neureuther (verantw.), Gundo Sanders, Steven Seeber, Michael Stölting

Anzeigenvertretung:
Medienmarketing SANDERS
Tel. o 72 03/50 27 270
Mail: gsanders@mm-sanders.de

Layout:
AD&D Werbeagentur GmbH,
Silvia Romann, Dietmar Kraus

Druck: Niederösterreichisches Pressehaus Druck- und Verlagsgesellschaft m.b.H., St. Pölten

Druckauflage: 52.500
Tatsächliche Verbreitung: 52.028 (IV/19)

Auflage und Verbreitung kontrolliert.

36. Jahrgang
Erscheinungsweise: 10 x jährlich

Abo-Preis:
29,– € p.a. plus Porto inkl. MwSt.

Einzelpreis: 2,90 €
Ein Abonnement verlängert sich automatisch um ein Jahr, wenn es nicht spätestens 3 Monate vor Ablauf des Bezugszeitraumes gekündigt wird.

ISSN 0931-4679
Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) Berlin

Zur Zeit gilt die Anzeigenpreisliste Nr. 37 vom 01.11.2019.

Titelkopf: © Fotolia.de/yellowj