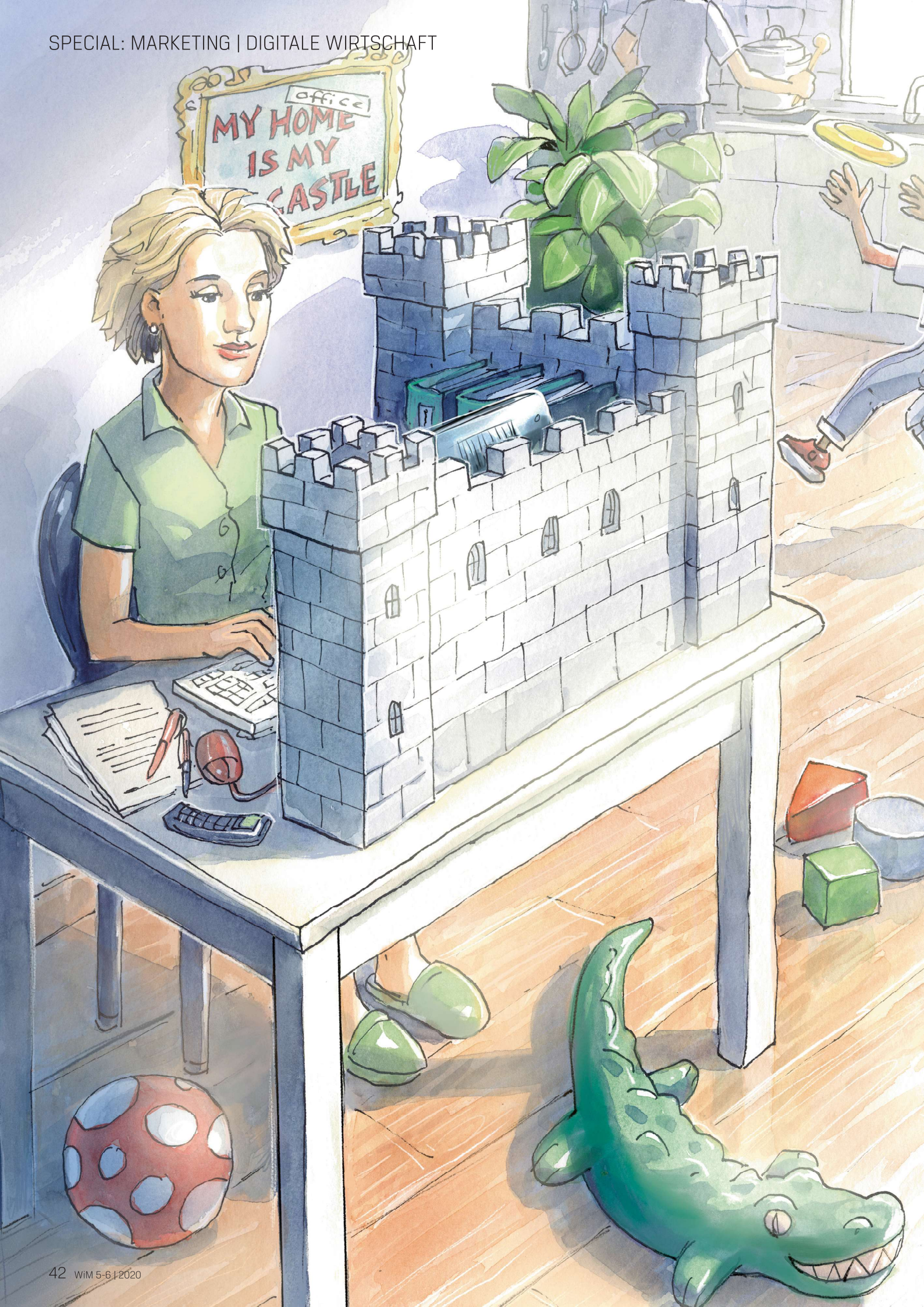
office
MY HOME
IS MY
CASTLE

HOME-OFFICE

Eine feste Burg

Vom heimischen Arbeitszimmer sicher auf die betrieblichen Daten zugreifen: Was ist beim Home-Office technisch zu beachten?

Von Patrick Oliver Graf; Illustration: Anton Atzenhofer

Abstand halten, Teams aufteilen: Dies ist in vielen Unternehmen das Gebot der Stunde, um die Mitarbeiter vor einer Ansteckung mit dem Corona-Virus zu schützen und um die Arbeitsfähigkeit des Betriebs sicherzustellen. Vielfach lässt sich dies dadurch erreichen, dass die Mitarbeiter ganz oder teilweise von zuhause arbeiten. Betriebe, in denen diese Form des Arbeitens bislang nicht üblich war, sehen sich damit vor eine Reihe von Herausforderungen gestellt – beispielsweise was Arbeitsorganisation, Mitarbeiterführung und Arbeitsrecht angeht. Insbesondere müssen sie auch für einen sicheren Zugriff auf die betrieblichen Daten sorgen. Was ist dabei zu beachten?

Technische Ausstattung

Wesentlich für das sichere Arbeiten im heimischen Arbeitszimmer ist die Ausstattung mit der geeigneten Technik. Die Corona-Krise hat gezeigt, dass viele Unternehmen nicht auf ein solches Krisenszenario vorbereitet waren und deshalb kurzfristig für die notwendige Infrastruktur sorgen mussten. Das war mitunter schwierig, weil die Hardware angesichts der hohen Nachfrage und der Corona-bedingten Lieferprobleme nur schwer und auch oft nur zu hohen Preisen zu beschaffen war. Auch die notwendigen Vorkehrungen für die Datensicherheit mussten oft kurzfristig getroffen werden. Deshalb sollte die aktuelle Krise zum Anlass genommen werden, ein Home-Office-Konzept auszuarbeiten.

Viele Wege führen ans Ziel

Es gibt viele Wege, um für eine sichere IT im heimischen Büro zu sorgen – sicher und effizient sollen sie aber sein. In der Regel stellt der Arbeitgeber für das Home-Office Endgeräte wie Notebooks und Tablets zur Verfügung, die auch für das mobile Arbeiten geeignet sind. Desktop-PCs sind für diesen Zweck kaum üblich, weil sie schwer transportierbar sind und weil Aufbau und Verkabelung aufwändig sind. Smartphones sind aufgrund der kleinen Displays und der kleinen virtuellen Tastaturen für das produktive Arbeiten im heimischen Arbeitszimmer ungeeignet, zudem fehlen hier in der Regel auch die anwendungsspezifischen Programme. Es sollte selbstverständlich sein, dass die zur Verfügung gestellten Geräte hinsichtlich der Version des Betriebssystems und der Einstellungen der sogenannten „Endpoint-Security", also der gesamten sicherheitsrelevanten Konfigurationen, immer auf dem aktuellen Stand sind. Zudem sollten auch die verwendeten Programme regelmäßig aktualisiert werden. Dadurch ist ein Angriff mit Schadsoftware, wie z. B. Viren und Ransomware, vermeidbar.

Viele Unternehmen lassen ihre Mitarbeiter noch an einem klassischen Desktop-PC arbeiten, was das Problem der Mobilität und der Reaktionsschnelligkeit im Krisenfall verstärkt. Der Desktop-PC, der in der Regel eine Dockingstation und einen externen Monitor angeschlossen hat, ist nachvollziehbar unhandlich und für einen spontanen Umzug des Arbeitsplatzes in das Home-Office ungeeignet. Unternehmen sind daher gut beraten, auch die Hardware-Ausstattung ihrer Mitarbeiter auf mögliche, künftige Vorkommnisse auszurichten. Es muss nicht immer gleich eine Pandemie sein, um Mitarbeiter im Home-Office zu belassen, beispielsweise können auch Unwetter mit massiven Verkehrsbehinderungen ein Grund dafür sein, wie die letzten Monate gezeigt haben. Unternehmen sind jetzt gefordert, eine langfristige Strategie zu etablieren, in der sowohl die Mitarbeiter im Home-Office als auch die dafür notwendigen netzwerktechnischen Ressourcen (wie z. B. leistungsfähige Server) Berücksichtigung finden. Letztere bilden eine wichtige Grundlage für eine erfolgreiche Home-Office-Strategie, um im Notfall schnell reagieren zu können.

Nur in Ausnahmefällen findet ein privater PC Verwendung, denn im Home-Office mangelt es diesem doch meist an den vom Unternehmen definierten Sicherheitsstandards wie beispielsweise Festplatten-Verschlüsselung oder Anti-Schadsoftware. Oder es befinden sich Programme und Daten auf dem PC, die bei einer Anbindung an das Unternehmensnetzwerk größeren Schaden anrichten könnten. Unternehmenseigene Geräte wie Lap-

tops unterliegen allen sicherheitsrelevanten Einstellungen und sind daher für einen Einsatz im Home-Office auf jeden Fall vorzuziehen. Sie verfügen über vorkonfigurierte Mechanismen, um alle sicherheitsrelevanten Einstellungen stets aktuell zu halten. Eine Installation von „privaten" Programmen muss ausgeschlossen sein, Gleiches gilt auch für eine freie Verwendung der USB-Schnittstellen.

Sichere VPN-Lösung

Ein wichtiges Instrument, um im Home-Office sicher arbeiten zu können, ist eine VPN-Software (Virtual Private Network), die auf den entsprechenden Endgeräten installiert wird. Sie stellt eine ideale Möglichkeit dar, um einen sicheren Austausch von Daten zwischen dem Anwender und dem Firmennetzwerk zu ermöglichen. Dies ist in Zeiten stark wachsender Cyberkriminalität geboten, in denen die Ansprüche an die Netzsicherheit sehr hoch sind. Bei VPN handelt es sich um eine Kommunikations- bzw. Netzwerktechnologie, die z. B. über ein öffentliches Netzwerk (Internet) eine sichere Verbindung herstellt. Die Daten werden durch einen sogenannten VPN-Tunnel verschlüsselt übertragen und sind dadurch geschützt. Bei intelligenten VPN-Lösungen kann auch unterschieden werden, welche Daten über den VPN-Tunnel übertragen werden sollen und welche nicht. Stichwort: Split-Tunneling, also die Trennung von geschäftlicher und privater Kommunikation.

Bei der Auswahl des Anbieters ist darauf zu achten, dass die VPN-Komponenten in die IT-Infrastruktur des Unternehmens integrierbar und mit den vorhandenen Netzwerkkomponenten kompatibel sind. Dies bedeutet wiederum einen deutlichen Investitionsschutz. Konkret heißt das, dass bestehende Komponenten weiterverwendet werden können, wie die VPN-Server-Landschaft oder sogenannte Token zur sicheren Authentifizierung. Vorzugsweise kommt eine reine Software-Lösung zum Einsatz, die auf der Anwenderseite die wichtigsten Betriebssysteme abdeckt (Windows, macOS, Linux, ergänzend iOS und Android) und deren Kommunikationskomponenten im Unternehmensnetzwerk sowohl auf virtuellen als auch auf klassischen Servern eingesetzt werden können. Besonders wichtig ist hier, dass sich die ausgewählte Lösung außerdem durch eine hohe Skalierbarkeit auszeichnet. Sie sollte sich also beliebig und schnell erweitern lassen, sodass im Notfall in kürzester Zeit selbst eine große Zahl weiterer Mitarbeiter in das Home-Office geschickt werden kann.

Häufig ist die Meinung anzutreffen, dass solche sicheren Lösungen zu komplex und somit auch zu kompliziert seien und vom Anwender zu viel technisches Wissen erforderten. Dies trifft sicher für einige Lösungen zu, nicht aber für komplett vorkonfigurierte, ganzheitliche VPN-Lösungen, bei denen die Mitarbeiter lediglich mit einem Mausklick eine sichere Verbindung herstellen. Weder müssen sie die Verbindung umständlich selbst konfigurieren, noch können sie an den vorkonfigurierten Einstellungen etwas verändern. Das ist einerseits ein wichtiger, sicherheitsrelevanter Aspekt und andererseits auch aus administrativer Sicht von Vorteil, weil die Betreuung deutlich einfacher ist und damit auch betriebliche Ressourcen schont. Intelligente VPN-Lösungen beinhalten also ein zentrales Konfigurations- und Rechtemanagement, in dem die Systemadministratoren die notwendigen Einstellungen vornehmen. Solche VPN-Systeme ermöglichen auch das Konfigurieren sogenannter „Endpoint-Policies" für ein sicheres Arbeiten – das bedeutet unter anderem, dass sich der Anwender mit dem Endgerät nur dann anmelden kann, wenn das Gerät vollumfänglich „up to date" ist.

Neben allen technischen Herausforderungen darf eines nicht vergessen werden: Wegen des dezentralen Arbeitens ist eine gute und enge Mitarbeiterführung immens wichtig. Diese darf nicht als Überwachung verstanden werden und das muss auch klar kommuniziert werden. Hat man dies nicht im Blick, besteht durchaus die Gefahr, dass der Mitarbeiter die Bindung zum Unternehmen verliert und darunter nicht nur die Produktivität leidet, sondern noch ganz andere Probleme, vor allem im zwischenmenschlichen Bereich, entstehen.

Hin und wieder äußern Unternehmen Vorbehalte in Bezug auf die Arbeit im Home-Office, weil sie Probleme mit Technik und Datensicherheit befürchten. Diese lassen sich leicht entkräften, wenn die genannten technischen Maßnahmen ergriffen werden. Ein nicht zu unterschätzender „weicher" Faktor ist am Ende der gesamten Kette der Mitarbeiter selbst. Eine gute Schulung zu Fragen der IT-Sicherheit und eine transparente interne Kommunikation sind mit entscheidend, um das Arbeiten im Home-Office für alle Seiten erfolgreich und produktiv zu gestalten.

Patrick Oliver Graf ist Geschäftsführer der NCP engineering GmbH in Nürnberg, die auf Lösungen für die sichere Daten-Kommunikation spezialisiert ist (www.ncp-e.com).

i

IHK-Infos zum Home-Office

Die IHK Nürnberg für Mittelfranken hat auf ihrer Homepage umfangreiche Informationen rund um das Home-Office zusammengestellt. Unter www.ihk-nuernberg.de/corona-homeoffice sind u. a. Tipps zu folgenden Themen abrufbar: arbeitsrechtliche und steuerliche Fragen zum Home-Office, Arbeitssicherheit, Datenschutz, technische Voraussetzungen und nützliche Links.

www.ihk-nuernberg.de/corona-homeoffice