



**Nostalgie:** Retrotrikots erinnern an die Geschichte des (Schweizer) Radsports. Im Vordergrund das Testrennvelo Min.D der Marke Open.

# Das Sicherheitsrisiko

Bei der Verlagerung ins Homeoffice sollten Firmen das **Netzwerk** in den Wohnstuben genauso professionell betreiben wie im Office.

PHILIPP KLOMP

Viele Unternehmen haben auch nach der behördlichen Aufhebung der Homeoffice-Pflicht die Heimarbeit als Option beibehalten. Sei dies, weil seitens der Arbeitnehmenden ein verstärkter Druck zu mehr Flexibilität der Arbeitseinteilung spürbar wurde, sei dies, weil sich damit das Wachstum ohne zusätzliches Anmieten von teuren Büroflächen bewerkstelligen lässt. Damit einher geht aber auch die Notwendigkeit, die technische Situation einmal grundlegend zu beurteilen. Denn anders als während der Verordnung der Heimarbeit durch den Bundesrat können in einer Post-Corona-Situation die durch die Pandemie bedingten Unwägbarkeiten nicht mehr so einfach entschuldigt werden. Wenn heute Videokonferenzen zu Performance-Problemen der IT oder die Nutzung der privaten Heimnetze für geschäftliche Belange zu Sicherheitsproblemen und Ausfällen führen, können für das Unternehmen gravierende Reputati-

onsschäden entstehen. Vom Verlust von Kundendaten oder von geistigem Eigentum ganz zu schweigen.

## Sinkender Einfluss auf IT

In einer Situation ohne Homeoffice sind die Rollen der Informatik üblicherweise klar: Die interne IT-Abteilung oder ein externer Dienstleister kümmert sich um die Verteilung und Verwaltung der Endgeräte wie Smartphones, Laptops und PC. Dabei versteht sich von selbst, dass neben den firmeneigenen auch private Geräte gemanagt werden. Auch wenn bei diesem Mix sicher bei vielen Unternehmen noch Verbesserungspotenzial hinsichtlich der Sicherheit besteht, so ist die Situation doch mehrheitlich transparent und die Aufgabenverteilung klar definiert. Anders aber bei der hybriden Nutzung von Büro- und Heimarbeitsplatz. Die IT des Arbeitgebers hat nämlich höchstens einen limitierten, meistens aber gar keinen Einfluss auf die Situation am Heimarbeitsplatz. Denn die Belegschaft arbeitet mit ihren Büro-PC und Smartphones in privaten Heimnetz-

werken. Videositzungen erfordern aber ein stabiles Netzwerk. Ruckelt es während der Videokonferenz mit den Kunden oder Lieferanten, so können sich interne IT und der Internetanbieter des privaten Anschlusses den Schwarzen Peter gegenseitig in die Schuhe schieben. Der Ruf der Firma leidet trotzdem, und

## Empfehlenswert ist ein Access Point, der vom Unternehmen verwaltet wird.

zwar beim Mitarbeitenden wie auch bei externen Partnern. Denn das Heimbüro beschränkt sich normalerweise nicht auf einen fixen Arbeitsplatz. Gearbeitet wird im gesamten Haushalt. Auch im Wohnzimmer, auf der Terrasse oder sonst wo teilt man sich mit Familienmitgliedern und Besuchern dasselbe Netz. Zusätzlich hängen immer häufiger am Internet angeschlossene Smart-Home-Geräte am selben Drahtlosnetz. Gerade bei Letzteren wird in den meisten Fällen Software,

die für grundlegende Funktionen von internetfähigen Lampen, Lautsprechern oder anderen Haushaltsgeräten in die Systeme eingebettet ist, von den Anwendern nicht auf dem neuesten Stand gehalten. So drohen neben Verzögerungen und Instabilität auch noch böswilliger Datenklau von aussen.

## Privat und Geschäft unbedingt trennen

Ebenso wie die ungenügende Abgrenzung bei den Mitarbeitenden von Berufs- und Privatleben für Unternehmen ein Stolperstein des Homeoffice sein kann, stellt sich auch eine unsaubere Trennung auf technischer Ebene als Herausforderung dar. Denn mangelnde persönliche Eignung für den Umgang mit grösserer zeitlicher und inhaltlicher Autonomie bei Mitarbeitenden sowie fehlende oder unklare Regeln dafür haben ihre Entsprechung beim IT-Teil des Homeoffice. Ohne diesen aber lässt sich die digitale Entsprechung des Büroarbeitsplatzes in den vier Wänden der Mitarbeitenden nicht professionell umsetzen. Empfehlenswerter ist ein extra Zugangspunkt (Access Point),

der im Gegensatz zum Heim-Router der Mitarbeitenden vom Arbeitgeber verwaltet wird. Die Arbeitsgeräte der Mitarbeitenden können dann lediglich und ohne technische Vorkenntnisse durch den Laien über die entsprechende Hardware am Internet angeschlossen werden. Dabei ist es von Vorteil, wenn der (interne oder externe) Dienstleister, der für das Management der Endpunkte (Geräte) zuständig ist, sich auch um die Verwaltung des geschäftlichen Teils des Heimnetzes kümmert. Gerade bei Unternehmen mit einer Cloud-First-Strategie, aber auch schon, wenn hybride Teile der Unternehmens-IT in der Cloud vorgehalten werden, macht es aus technischer Sicht wenig Sinn, den Netzwerkverkehr via virtuelles privates Netz (VPN) in die Firmen-Ressourcen hinein und von dort wieder zurück ins Homeoffice zu lenken. Aus den genannten Gründen ist es ratsam, den Traffic durch entsprechende Netzwerkkomponenten direkt via Internet in die Cloud zu steuern und abzusichern.

Philipp Klomp, CEO Nomasis, Zürich.

ANZEIGE

## Der Schweiz verpflichtet.

Wir fördern mit unseren unternehmerischen Aktivitäten und aus deren Erträgen das Unternehmertum und die Innovation in der Schweiz.

**Treten Sie mit uns in Kontakt.**

**F.G. PFISTER**  
holding ag

[www.pfisterholding.ch](http://www.pfisterholding.ch)